UNIVERSIDAD NACIONAL DE LA PLATA

FACULTAD DE CIENCIAS EXACTAS

DEPARTAMENTO DE FISICA

Trabajo de Tesis Doctoral:

Holografía digital 3D y su extensión a la encriptación óptica, la compresibilidad y la visualización de la información

---

Tesista:

Alejandro Velez Zea

Director:

Dr. Roberto Torroba

Año:

2018

Contenidos

Introducción

En el año 1826 la humanidad dio un enorme salto en su capacidad de registrar la historia y el conocimiento colectivo. En este año, Joseph Nicéphore Niépce realiza el primer heliograbado, logrando registrar una imagen de paisaje visible desde su ventana. De esta manera, por primera vez disponemos de una forma de registrar imágenes del mundo real sin recurrir a la pintura u otras expresiones artísticas. El subsecuente desarrollo de la fotografía ha hecho posible nuevas formas de transmisión de información difícil de plasmar en un texto.

Sin embargo, la fotografía tradicional es una proyección bidimensional de un mundo tridimensional, y a pesar de que se puede generar la ilusión de profundidad por medio de la perspectiva o la estereoscopia, no es sino hasta 1947 cuando se encontró un método para registrar toda la información presente en una escena. Este método fue llamado "holografía" por el hombre que lo descubrió, Dennis Gabor [1].

La holografía permite capturar la información de un objeto tridimensional, por medio del diagrama de interferencia entre la luz dispersada por el objeto y un haz de referencia, el cual es comúnmente llamado "holograma".

El descubrimiento de la holografía y las potenciales aplicaciones de la misma, fueron objeto de enorme interés por parte de la comunidad de la óptica durante la segunda mitad del siglo XX. Sin embargo, los retos a los que se enfrentaron los investigadores en el desarrollo de los métodos holográficos fueron tan variados como difíciles de resolver.

Paralelamente a estos esfuerzos, se dio la gran revolución de las telecomunicaciones y la computación, con el crecimiento vertiginoso del internet y de la capacidad de procesamiento disponible.

El desarrollo de la holografía digital, es decir, del registro de información holográfica por medios digitales, responde en buena medida a la necesidad de tender puentes entre el dominio de la óptica y el de los sistemas digitales modernos. Los sistemas opto-digitales

resultantes, dan lugar a novedosas e interesantes aplicaciones, que se alimentan de los desarrollos en ambos campos y permiten subsanar las dificultades a los que se enfrentan cada uno.

De esta manera, algunas de las limitaciones propias de la holografía pudieron ser paulatinamente mitigadas, con elementos electrónicos capaces de registrar hologramas de objetos más detallados y computadoras capaces de reconstruir, procesar, e incluso generar información holográfica con crecientes niveles de complejidad.

Un ejemplo claro de esta feliz unión entre lo óptico y lo digital lo encontramos en el estudio de la encriptación óptica. La encriptación óptica ofrece una alternativa a los métodos clásicos de encriptación basados en sistemas digitales, con el potencial de ofrecer mayor seguridad, velocidad y economía. Varios de los criptosistemas ópticos más estudiados son en esencia sistemas holográficos, por lo que las técnicas de la holografía tradicional son aplicables a estos sin necesidad de alteraciones significativas. Adicionalmente, conforme aumentan los volúmenes de información intercambiados en las sociedades modernas, y al ser la criptografía digital un área relativamente madura, las alternativas ópticas cobran mayor interés.

Por otro lado, la capacidad de registrar digitalmente hologramas de mayor resolución nos plantea el problema de cómo manejar el creciente volumen de la información holográfica resultante de forma eficiente. Encontrar solución a este problema se hace especialmente importante al tener en cuenta que los métodos digitales de compresión están optimizados para las características particulares de los datos comúnmente almacenados en las computadoras, como lo son los caracteres o las imágenes.

En este sentido, no es un planteamiento descabellado suponer que los métodos ópticos tal vez sean los mejores adaptados para lograr la compresión de datos holográficos. Así, es necesario entender exactamente cuáles son las características de esta información, para así diseñar estrategias óptimas que permitan su procesado, ya sea por medios digitales u ópticos.

Finalmente, los avances en los moduladores espaciales de luz hacen posible la visualización de información holográfica con un nivel de precisión que era imposible hasta hace pocos años, resultando en toda una nueva familia de aplicaciones que van

desde la micro manipulación óptica hasta la posibilidad de crear displays holográficos con reconstrucción de objetos 3D en tiempo real.

Este trabajo de tesis está planteado como un estudio del estado del arte actual de las aplicaciones de la holografía digital arriba mencionadas, es decir, la encriptación óptica, la compresión y la visualización de datos holográficos. Conforme recorremos estas temáticas, nos encontramos con algunas de las limitaciones de las técnicas actuales, realizando en varios casos propuestas novedosas para mitigar o dar solución a las mismas. De esta manera, no nos abocamos a la solución de un problema específico, si no a la extensión de las capacidades de la holografía digital para la solución de problemas en las aplicaciones que de ella emanan.

Por supuesto, cada uno de los temas aquí expuestos es en sí mismo digno de estudio especializado, sin embargo, la generalidad con la que trataremos los temas nos permitirá mostrar la íntima relación que existe entre diversas técnicas que usualmente son presentada de forma aislada para cada aplicación, y de esa manera asegurar que nuestras propuestas tengan aplicabilidad más allá del problema inmediato al que se le pretende dar respuesta.

Así pues, hemos divido nuestro trabajo en cuatro capítulos, el primero de los cuales introduce los principios generales de la holografía digital. En este capítulo presentamos el formalismo matemático básico que da cuenta del fenómeno holográfico, así como la discretización de esta formulación que resulta del uso de medios de registro digitales, como lo son las cámaras CCD o CMOS. Introduciremos también la holografía de Fourier como una alternativa a la holografía de Fresnel, explicando a grandes rasgos las ventajas y desventajas de cada una de ellas. Posteriormente, explicaremos las condiciones mínimas para un registro digital adecuado de la información holográfica, teniendo en cuenta la frecuencia de las franjas de interferencia, el tamaño y resolución de la cámara y su rango dinámico. Luego expondremos el proceso de filtrado, con el cual se elimina información redundante y no deseada del holograma. A continuación, haremos una breve reseña del multiplexado holográfico, centrándonos en el multiplexado espacial y demostrando su efectividad para ensamblar escenas holográficas cuya extensión supera las limitaciones del sistema de registro.

También exploramos los sistemas de holografía a color, explicando la importancia de la elección de las fuentes de iluminación y como se determina el espacio de color a partir

de esta elección. Luego, discutimos las alternativas para registrar los hologramas a color, usando una cámara a color con filtro Bayer o registrando cada color por separado, explicando el procesamiento necesario para la reconstrucción optima de los objetos a color a partir de los hologramas registrados.

Finalmente, discutimos la importancia relativa de la fase y la amplitud para la reconstrucción a partir de la información holográfica.

En el segundo capítulo, introducimos la encriptación óptica de doble mascara de fase aleatoria, mostrando la relación entre los correladores ópticos, los sistemas holográficos y la encriptación. Tras establecer esta relación, introducimos el correlador de transformada conjunta, y presentamos estudios en los que analizamos el desempeño de criptosistemas derivados del mismo, como una contribución novedosa al estudio del área. Luego, enumeramos los distintos tipos de vulnerabilidades que sufren estos métodos, mostrando una técnica con el potencial de mitigar o eliminar completamente algunas de estas vulnerabilidades.

Luego, exploramos el problema del ruido en los criptosistemas ópticos, mostrando una de las estrategias para evitar los efectos nocivos del mismo sobre la información cifrada: los denominados “contenedores de información”. De manera seguida, introducimos un nuevo diseño de contenedor que presenta un mejor rendimiento que los empleados hasta el momento en la literatura.

A continuación, abordamos directamente el problema del ruido, exponiendo algunas de las técnicas propuestas para reducirlo, y posteriormente analizándolo en detalle, dando como resultado de este análisis una técnica capaz de lograr una alta reducción de la degradación en los objetos desencriptados. Posteriormente, extendemos el análisis de las fuentes de ruido para incluir otros factores únicos a las implementaciones experimentales de los criptosistemas, demostrando un protocolo compuesto de múltiples técnicas, algunas conocidas y otras desarrolladas por nosotros, que resultan en un aumento significativo del desempeño de los métodos experimentales de encriptación ópticos.

Como ultima sección de este capítulo, demostramos por primera vez la capacidad de los criptosistemas ópticos de procesar información 3D usando como llaves otros datos 3D, capacidad que de nuevo demuestra la conexión entre la holografía digital y la

encriptación, y con potenciales aplicaciones a la protección de contenidos holográficos en futuros sistemas de visualización basados en estas técnicas.

En el capítulo III, estudiamos los detalles del almacenamiento de los registros holográficos en medios digitales, y las técnicas tradicionales empleadas para lograr compresión de esta información, haciendo especial énfasis en las limitaciones de las mismas. Como respuesta original a estas limitaciones, proponemos dos métodos de compresión con perdida basados en sistemas ópticos. El primero de estos métodos realiza un escalado por medio de una lente convergente, logrando así reducir el espacio necesario para el registro holográfico. Posteriormente, mostramos que una combinación de técnicas digitales y técnicas ópticas puede dar lugar a un método de compresión y multiplexado, en el cual varios hologramas son empaquetados en el mismo espacio que ocuparía uno solo, con la posibilidad de lograr posteriormente la reconstrucción selectiva de cualquiera de los hologramas registrados. Finalmente, evaluamos el desempeño de nuestras propuestas por medio de comparaciones con técnicas estándar de compresión como lo son el JPEG. En este sentido, analizamos el comportamiento de la amplitud y la fase por separado, y demostramos la efectividad de los procesos ópticos para lograr una reducción de volumen de los hologramas digitales y de la información encriptada ópticamente.

En el último capítulo, abordamos la visualización óptica de información holográfica almacenada digitalmente, por medio del uso de moduladores espaciales de luz de solo fase. Una parte importante del desarrollo moderno de la holografía se centra en esta área, gracias a que estos nuevos elementos plantean la posibilidad de controlar los campos ópticos con un elevado grado de flexibilidad, lo que encuentra aplicaciones de diversa índole, desde la construcción de displays holográficos capaces de proyectar escenas tridimensionales hasta trampas ópticas para la manipulación de nanopartículas. Animados por este gran abanico de posibilidades, realizamos una introducción básica a los sistemas de visualización. Posteriormente, mostramos el procesamiento necesario para reconstruir hologramas digitales usando estos elementos de forma exitosa y explicamos algunas de las limitaciones tecnológicas propias de los mismos

A continuación, estudiamos algunas de las técnicas usadas para la generación de hologramas por computadora, centrando nuestro estudio en hologramas de imágenes de amplitud 2D. En esta temática, introducimos también un nuevo método, basado en la

combinación de técnicas clásicas de generación de hologramas, el cual tiene el potencial de generar grandes cantidades de hologramas de manera rápida y eficiente, capacidad de gran utilidad en aplicaciones en las cuales se busca un control dinámico de los campos luminosos, como lo sería la generación de videos holográficos o la micro manipulación de nanopartículas en tiempo real.

Finalmente, discutimos las complejidades propias de la implementación de sistemas de visualización holográfica a color, demostrando experimentalmente la construcción de un sistema de este tipo y por primera vez en la literatura, su uso para la reconstrucción de información holográfica comprimida a color.

Tras estos cuatro capítulos, realizamos una compilación de las conclusiones alcanzadas en el estudio de las temáticas expuestas y de las posibles consecuencias de las propuestas originales aquí contenidas, con miras a futuras investigaciones que resulten en la posibilidad de nuevas áreas de aplicación o en el aumento de las capacidades actuales de la holografía digital.

I. Principios de la holografía digital

1.1. Introducción.

Un holograma es esencialmente un diagrama de interferencia entre dos ondas, donde una de las cuales es la luz dispersada por un objeto o escena y la otra es una onda de referencia. Aunque estos diagramas de interferencia son usualmente registrados por medios bidimensionales, como películas fotográficas, o cámaras digitales, contienen información tridimensional sobre la escena que dispersa la luz. El nombre de holograma está bien fundado, al provenir de la unión de la palabra griega "holos" que significa "entero" o "completo" y "graphein" que significa "escribir". Así, un holograma es el registro completo de un objeto.

El concepto de holografía ha sido ha sido extendido de diversas maneras, entre la cuales nos encontramos con la holografía digital. La holografía digital, es decir, usar medios digitales para registrar datos holográficos, fue introducido por primera vez en 1967 [2]. A pesar de la evidente utilidad de los medios digitales para el registro de hologramas, los primeros desarrollos sufrían las serias limitaciones de la electrónica de la época. Los sensores CDD, y en general las cámaras digitales, están compuestos de un número finito de celdas fotosensibles, llamadas pixeles (del inglés picture element), que registran la intensidad del campo incidente y ocupan unas dimensiones finitas. Los primeros sensores usados tenían pixeles de gran tamaño, relativamente baja área activa, y eran arreglos unidimensionales, lo que hacía necesario múltiples registros para obtener un solo holograma. Por otro lado, la limitada capacidad de computo disponible para la reconstrucción de los hologramas digitales limitaba las posibilidades de realizar un procesamiento digital de los mismos. Dadas estas dificultades, la holografía con películas era más atractiva para gran cantidad de aplicaciones.

Con el paso de los años, y los vertiginosos avances en capacidad de cómputo y fabricación de semiconductores, el panorama ha cambiado significativamente. Las

cámaras digitales CCD y CMOS se han convertido en un componente ubicuo en los celulares, tablets y laptops modernos, con tamaños de pixel del orden de los micrones. Esto hace posible el registro de hologramas de objetos complejos con sensores de bajo costo. Por otro lado, la reconstrucción de hologramas puede llevarse a cabo en tiempo real gracias a los poderosos procesadores multinúcleo disponibles actualmente.

De esta manera, las aplicaciones de la holografía digital se han multiplicado, abarcando displays holográficos 3D, microscopios holográficos y una gran variedad de técnicas de metrología interferométrica. En particular, la holografía digital permite registrar, almacenar y procesar grandes cantidades de datos holográficos, lo que era difícil de lograr usando la holografía en películas o con cristales fotorrefractivos. La mayoría de los sistemas de holografía digital solo difieren de los sistemas clásicos en el uso de cámaras digitales como medio de registro, y están compuestos de algún tipo de interferómetro, en el que un brazo está libre de elementos ópticos y provee la onda de referencia, y el otro ilumina el objeto a registrar, ya sea por transmisión o reflexión.

La clasificación de los sistemas de registro holográfico normalmente se hace con base en la orientación con la que incide la onda de referencia sobre el medio de registro y la transformación que sufre la luz proveniente del objeto antes de llegar a dicho medio. Respecto a la orientación de la onda de referencia, los sistemas holográficos se dividen en la configuración original demostrada por Gabor [1], llamados sistemas en eje, donde la onda de referencia incide paralela a la onda proveniente del objeto. La otra configuración es denominada fuera de eje [3], donde la onda de referencia incide sobre el medio de registro con un ángulo pequeño respecto a la onda proveniente del objeto. Los sistemas fuera de eje tienen la ventaja de requerir un solo registro para obtener la fase y amplitud de la onda objeto, con la desventaja de un menor ancho de banda, debido a la mayor frecuencia de las franjas de interferencia. Los sistemas en eje permiten un ancho de banda mayor, con franjas de más baja frecuencia, sin embargo, el objeto reconstruido se superpone con una imagen real distorsionada y la luz de la onda de reconstrucción. Este efecto hace necesario el uso de múltiples registros y técnicas de corrimiento de fase [4–6] para lograr una reconstrucción satisfactoria, lo que limita las posibles aplicaciones del método.

Por otro lado, respecto a la trasformación a la que se somete la onda objeto, encontramos los llamados hologramas de Fourier, en los cuales el medio de registro

captura la transformada de Fourier de la onda objeto, obtenida usualmente con una lente convergente, y también encontramos los hologramas de Fresnel, donde la onda objeto se propaga libremente desde el objeto hasta el medio de registro. Esta propagación libre es descrita por una transformada de Fresnel, de ahí su nombre.

A pesar de los avances tecnológicos arriba expuestos, la holografía digital todavía presenta serias limitaciones. En particular, el tamaño de pixel y área activa de las cámaras digitales son inferiores a las películas holográficas, las cuales pueden registrar hologramas con frecuencias de hasta 5000 líneas/mm. Esto implica que el tamaño de las escenas que se desea registrar es limitado, obligando al uso de técnicas de multiplexado si se desean registrar escenas extensas. Adicionalmente, el poder de cómputo y la capacidad de memoria necesaria para almacenar y procesar hologramas crece rápidamente con la resolución de los mismos, lo que hace de gran interés el estudio de técnicas de compresión, para así lograr un uso más eficiente de los recursos computacionales.

La otra limitante de la holografía digital está asociada a los requerimientos de coherencia de la fuente de iluminación para garantizar una adecuada visibilidad de las franjas. Debido a estos requerimientos, es necesario usar fuentes de luz laser, lo que incrementa el costo y la complejidad del registro holográfico, en particular cuando se desea realizar holografía a color, caso en el cual tres o más láseres con distintas longitudes de onda son necesarios para el adecuado registro. Por otro lado, las cámaras digitales a color usan un filtro Bayer para registrar los distintos canales de color, lo que se traduce en una resolución efectiva menor que las cámaras monocromáticas.

Finalmente, si se desea reconstruir ópticamente un holograma digital, es necesario un elemento capaz de modular el campo óptico tanto en fase como en amplitud simultáneamente. Esto puede lograrse por medio de impresión litográfica, pero si se desea reconstrucción de varios hologramas, o de un video, es necesario un medio electrónico programable. En la práctica, no existen elementos electrónicos que puedan modular de forma simultánea e independiente tanto la amplitud y como la fase de un campo óptico. En particular, existen moduladores espaciales de luz de cristal líquido (SLM por la sigla en inglés de “spatial light modulator”) capaces de modular la amplitud o la fase del campo óptico, pero no ambos al mismo tiempo. Por otro lado, investigación en el área de análisis de señales y holografía, demostró que la fase contiene gran parte de

la información necesaria para reconstruir un objeto. Este hecho, combinado con las limitaciones de los SLM hace relevante el estudio de la holografía de solo fase, en la que se descarta la información de amplitud del holograma.

El propósito de este capítulo es introducir los principios básicos de la holografía digital fuera de eje, partiendo de la integral de Fresnel-Kirchoff, incluyendo la aproximación de Fresnel, el efecto de discretización causado por el registro digital, la reconstrucción de los hologramas digitales, el filtrado, y la eliminación del orden cero. Posteriormente se discutirá la holografía de solo fase, y se presentará el multiplexado espacial para reconstrucción de escenas extendidas. Por último, se demostrará el registro de hologramas a color con tres longitudes de onda.

1.2. Holografía de Fresnel.

Un esquema tradicional de holografía consta de una fuente de luz laser, un sistema de colimación que permite obtener un frente de onda plano, y un interferómetro, como un Michelson o Mach-Zenhder, el cual divide la luz proveniente de la fuente laser en dos ondas. Una de las ondas ilumina el objeto cuyo holograma se desea registrar, y la otra provee el haz de referencia. Un esquema básico para holografía de Fresnel se muestra en la Figura 1.

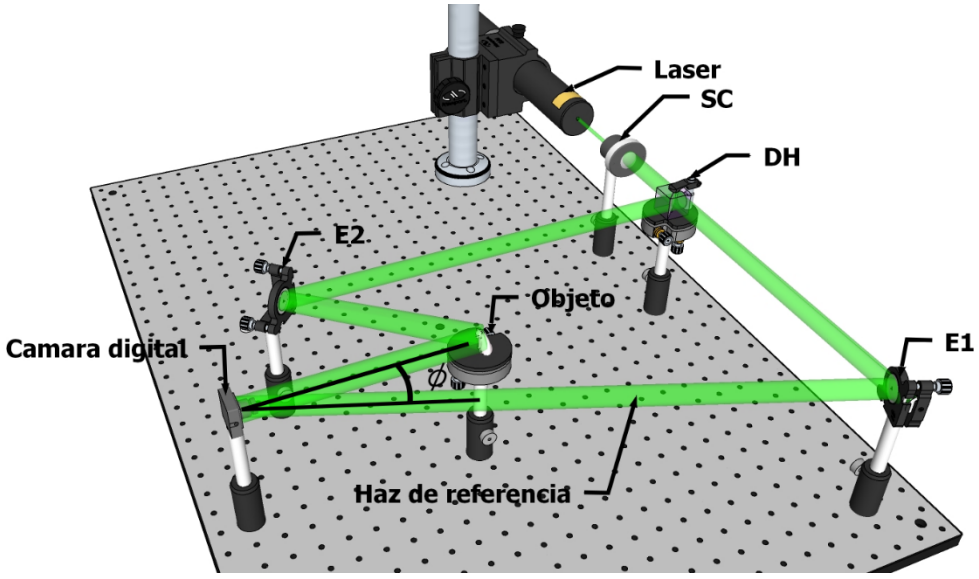

Figura 1: Esquema de un sistema de holografía de Fresnel fuera de eje. SC: Sistema de colimación, E: Espejo, DH: divisor de haz, ϕ ángulo de incidencia del haz de referencia.

La luz dispersada por el objeto se propaga una distancia d hasta el medio de registro, donde interfiere con el haz de referencia. Así pues, el holograma registrado está dado por [7]

$$h(x,y) = h_0 + \beta\tau I(x,y) \tag{1.2.1}$$

donde h_0 es la transmisión de amplitud del medio de registro, la cual para una cámara CCD o CMOS es 0, β es una constante que depende de la sensibilidad del medio de registro, τ es el tiempo de integración y finalmente $I(x,y)$ es la intensidad de la interferencia entre la onda objeto y la onda de referencia, dado por

$$\begin{aligned} I(x,y) = &| O(x,y) |^2 + | R(x,y) |^2 + \\ &O(x,y)R^*(x,y) + O^*(x,y)R(x,y) \end{aligned} \tag{1.2.2}$$

En la expresión anterior, $O(x,y)$ y $R(x,y)$ son funciones complejas que describen la onda objeto y la onda de referencia respectivamente. Para simplificar el tratamiento supondremos que tanto β como τ son iguales a la unidad, con lo que el holograma $h(x,y)$ es igual al patrón de interferencia $I(x,y)$. Si suponemos que el haz objeto incide perpendicularmente sobre el medio de registro y el haz de referencia incide con un ángulo ϕ, podemos escribir el haz de referencia como

$$R(x,y) = re^{-\frac{2\pi}{\lambda}i(x\sin\phi)} \tag{1.2.3}$$

donde λ es la longitud de onda y r es la amplitud constante del haz de referencia. Ahora bien, una vez se registra el holograma $h(x,y)$, para su reconstrucción es necesario iluminar el mismo con la onda de referencia. Así se obtiene

$$\begin{aligned} h(x,y)R(x,y) = &[| O(x,y) |^2 + r^2]re^{-\frac{2\pi}{\lambda}i(x\sin\phi)} \\ &+ r^2O(x,y) + r^2e^{-\frac{4\pi}{\lambda}i(x\sin\phi)}O^*(x,y) \end{aligned} \tag{1.2.4}$$

El primer término de la ecuación anterior es simplemente la onda de referencia multiplicada por un factor, y corresponde a la luz no difractada por el holograma. El segundo término es la onda objeto multiplicada por la amplitud de la onda de referencia, que influirá en el brillo del objeto reconstruido, y el tercer factor corresponde al complejo conjugado de la onda objeto. Los exponenciales complejos que aparecen multiplicando el

primer y tercer término son particulares de los sistemas de holografía fuera de eje, y resultaran en la separación espacial de los distintos términos en el plano de reconstrucción.

Tras iluminar el holograma con la onda de referencia, se obtiene una imagen virtual del objeto reconstruido a una distancia d detrás del holograma, y una imagen real a la misma distancia, pero en el sentido contrario, además de la luz no difractada. Las posiciones de estas imágenes respecto al centro del holograma dependerán del ángulo de incidencia y la distancia d, como se muestra en la Figura 2.

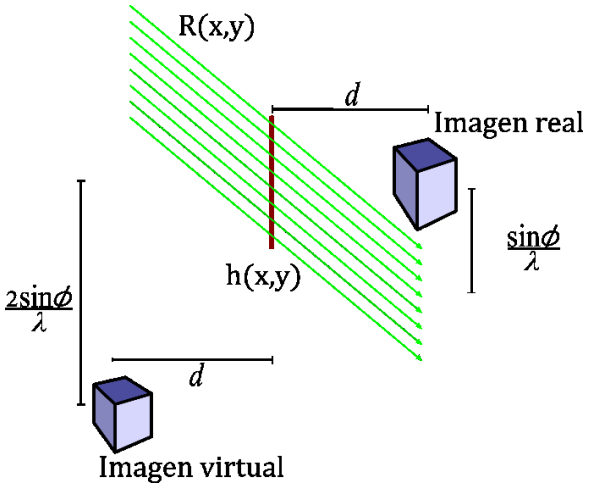

Figura 2: Esquema de la reconstrucción de un holograma fuera de eje.

Ahora bien, aunque la reconstrucción óptica solo requiere de la iluminación adecuada del holograma, para reconstruir el holograma digital este proceso debe ser descrito de manera que pueda ser llevado a cabo computacionalmente. Para ello primero es necesario describir la propagación de la luz desde el plano del holograma hasta el plano de reconstrucción que se encuentra a una distancia d. Esta propagación esta descrita por la integral de Fresnel-Kirchoff, dada por

$$\Gamma(\eta,\xi)=\frac{i}{\lambda}\int_{-\infty}^{\infty}\int_{-\infty}^{\infty}h(x,y)R(x,y)\frac{\exp\left(-i\frac{2\pi}{\lambda}\rho\right)}{\rho}\left(\frac{1}{2}+\frac{1}{2}\cos\theta\right)dxdy \qquad (1.2.5)$$

con

$$\rho=\sqrt{(x-\eta)^2+(y-\xi)^2+d^2} \qquad (1.2.6)$$

Donde ρ es la distancia entre un punto en el plano del holograma con coordenadas (x, y) y un punto en el plano de reconstrucción con coordenadas (η, ξ) , como se puede apreciar en la Figura 3.

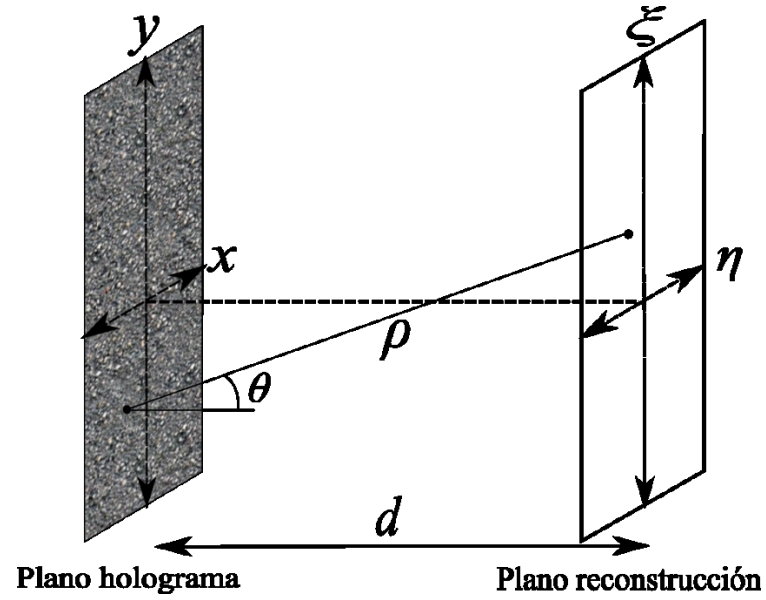

Figura 3: Sistema coordenado para la integral de Fresnel-Kirchoff.

Solucionando numéricamente la ecuación (1.2.5), es posible obtener la información de la amplitud y de la fase del objeto reconstruido. La solución numérica de la ecuación de Fresnel-Kirchoff es costosa en tiempo de cómputo, lo que la hace poco adecuada para la mayoría de las aplicaciones prácticas de la holografía digital.

Con el propósito de simplificar el cálculo de la reconstrucción, introducimos la aproximación de Fresnel. En esta aproximación, suponemos que los valores de las coordenadas (x, y) y (η, ξ) son pequeños comparados con la distancia d entre el plano del holograma y el plano de reconstrucción. Con esta suposición, reemplazamos la expresión (1.2.6) por el primer término de su expansión en series de Taylor.

$$\begin{aligned}\rho &= d + \frac{(\eta - x)^2}{2d} + \frac{(\xi - y)^2}{2d} - \frac{1}{8}\frac{\left[(\eta - x)^2 + (\xi - y)^2\right]}{d^3} + \dots \\ &\approx d + \frac{(\eta - x)^2}{2d} + \frac{(\xi - y)^2}{2d}\end{aligned} \qquad (1.2.7)$$

Esta aproximación es esencialmente la aproximación paraxial, por lo que también asumimos que $\cos\theta \approx 1$. Reemplazando estas aproximaciones y simplificando en la ecuación (1.2.5), obtenemos

$$\Gamma(\eta,\xi)=\frac{i}{\lambda d}\exp\left(-i\frac{2\pi}{\lambda}d\right)\exp\left(-i\frac{\pi}{\lambda d}(\eta^2+\xi^2)\right)$$
$$\int_{-\infty}^{\infty}\int_{-\infty}^{\infty}R(x,y)h(x,y)\exp\left[-i\frac{\pi}{\lambda d}(x^2+y^2)\right] \qquad (1.2.8)$$
$$\exp\left[i\frac{2\pi}{\lambda d}(x\eta+y\xi)\right]dxdy$$

La expresión anterior es la llamada transformada de Fresnel. Esta transformación se puede calcular numéricamente con facilidad, debido que es en esencia una transformada de Fourier con la adición de una función de transferencia dada por.

$$F(x,y)=\exp\left[-i\frac{\pi}{\lambda d}(x^2+y^2)\right] \qquad (1.2.9)$$

Así, el holograma reconstruido es dado por

$$\Gamma(\eta,\xi)=\frac{i}{\lambda d}\exp\left(-i\frac{2\pi}{\lambda}d\right)\exp\left(-i\frac{\pi}{\lambda d}(\eta^2+\xi^2)\right) \qquad (1.2.10)$$
$$TF\left\{R(x,y)h(x,y)F(x,y)\right\}$$

Donde $TF\{\ \}$ representa la operación transformada de Fourier. Esta ecuación puede ser resuelta de forma más eficiente que la integral de Fresnel-Kirchoff, sin embargo, hasta ahora hemos considerado el holograma y los campos ópticos como funciones continuas. Para poder realizar el cálculo numérico en la práctica, debemos tener en cuenta que los sistemas digitales son discretos. El tamaño y cantidad de pixeles en la cámara digital tiene el efecto de limitar el detalle y el tamaño máximo de los objetos que pueden ser registrados. Para poder reconstruir efectivamente el holograma, es necesario convertir la transformada de Fresnel en su equivalente discreto. Para ello, primero llevaremos a cabo el siguiente cambio de variables en la ecuación (1.2.8). Sea

$$v=\frac{\eta}{\lambda d};\quad \mu=\frac{\xi}{\lambda d} \qquad (1.2.11)$$

Entonces la ecuación (1.2.8) queda

$$\Gamma(v,\mu)=\frac{i}{\lambda d}\exp\left[-i\pi\lambda d\left(v^2+\mu^2\right)\right]$$
$$\int_{-\infty}^{\infty}\int_{-\infty}^{\infty}R(x,y)h(x,y)\exp\left[-i\frac{\pi}{\lambda d}(x^2+y^2)\right]\exp\left[2\pi i(xv+y\mu)\right]dxdy \qquad (1.2.12)$$

Suponiendo que nuestra cámara digital tenga $M \times N$ pixeles, con tamaño de pixel $\Delta x \times \Delta y$, podemos cambiar las integrales de la ecuación (1.2.8) por sumatorias, tal que

$$\Gamma(m,n) = \frac{i}{\lambda d}\exp\left[-i\pi\lambda d(m^2\Delta v^2 + n^2\Delta\mu^2)\right] \sum_{k=0}^{M-1}\sum_{l=0}^{N-1} R(k,l)h(k,l)\exp\left[-i\frac{\pi}{\lambda d}(k^2\Delta x^2 + l^2\Delta y^2)\right] \exp[i2\pi(k\Delta x m\Delta v + l\Delta y n\Delta\mu)] \quad (1.2.13)$$

Con $m = 0,1,...,M-1$ y $n = 0,1,...,N-1$ las coordenadas en pixeles. Adicionalmente, Δx , Δy y Δv , $\Delta\mu$ están relacionados de la forma

$$\Delta v = \frac{1}{M\Delta x}; \qquad \Delta\mu = \frac{1}{N\Delta y} \quad (1.2.14)$$

Finalmente, si remplazamos la relación anterior en la ecuación (1.2.13), obtenemos

$$\Gamma(m,n) = \frac{i}{\lambda d}\exp\left[-\pi i\lambda d\left(\frac{m^2}{M^2\Delta x^2} + \frac{n^2}{N^2\Delta y^2}\right)\right] \sum_{k=0}^{M-1}\sum_{l=0}^{N-1} R(k,l)h(k,l)\exp\left[-i\frac{\pi}{\lambda d}(k^2\Delta x^2 + l^2\Delta y^2)\right] \exp\left[2\pi i\left(\frac{km}{M} + \frac{ln}{N}\right)\right] \quad (1.2.15)$$

Que es la transformada discreta de Fresnel. Esta se puede resolver haciendo la transformada discreta de Fourier del producto $R(k,l)h(k,l)\exp\left[-i\,\pi/\lambda d(k^2\Delta x^2 + l^2\Delta y^2)\right]$, usando el algoritmo de transformada rápida de Fourier. Esta definición también permite mostrar que la transformada de Fresnel mantiene las propiedades de la transformadas de Fourier, como lo es el teorema de convolución.

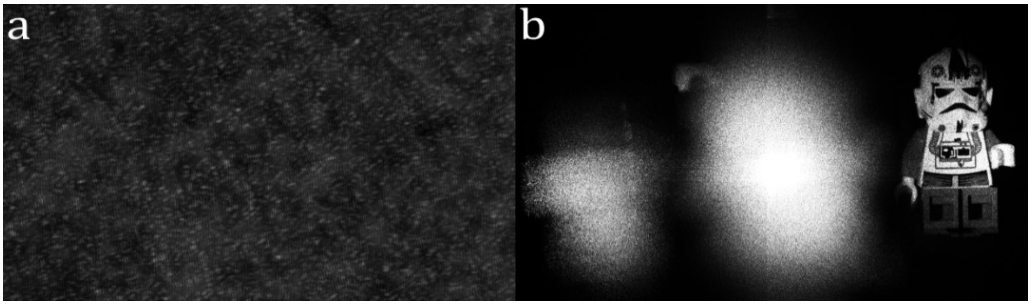

Figura 4: a) holograma de Fresnel fuera de eje, b) reconstrucción de a).

En la Figura 4, se muestra el ejemplo de un holograma de Fresnel registrado con un sistema como el de la Figura 1 y su respectiva reconstrucción digital. En la Figura 4b se puede apreciar el orden cero, y una nube de ruido, que corresponde a la imagen virtual desenfocada, además del objeto reconstruido. Este objeto fue registrado con una cámara CMOS de 3840x2748 pixeles de resolución, con un tamaño de pixel de 1.6 μm.

Para mostrar que un holograma contiene toda la información del campo óptico podemos considerar que para objetos 3D con profundidad extendida no existe un solo plano de reconstrucción. En este caso, podemos entender al objeto como una serie de secciones transversales, una detrás de otra. La sección más cercana del objeto al holograma estará a una distancia $d-\Delta d$ y la más lejana a $d+\Delta d$. A la hora de reconstruir, solo aparecerá bien enfocado la sección correspondiente a la distancia usada en la transformada de Fresnel, mientras que la reconstrucción de las secciones del objeto presentara una degradación conforme se alejen del plano de reconstrucción. Este comportamiento es similar al "enfoque" de una cámara con apertura limitada, sin embargo, a diferencia de una fotografía, que es un registro de intensidad, en un holograma tenemos la información completa del campo óptico, tanto en fase como en amplitud, lo que permite "enfocar" otra parte del objeto simplemente cambiando la distancia de reconstrucción en la transformada de Fresnel como se muestra en el gato de la Figura 5, sin necesidad de tomar un nuevo objeto.

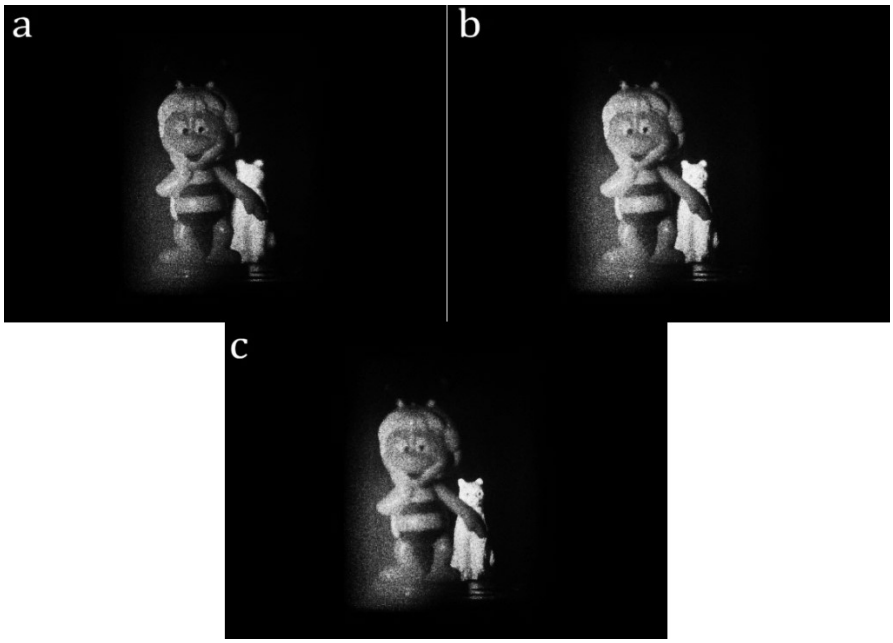

Figura 5: Reconstrucción de objeto 3D extendido en distintos planos. a) Plano cercano, b) plano medio, y c) plano lejano.

1.3. Holografía de Fourier

Es posible obtener una simplificación de la holografía de Fresnel cuando se ubica una lente entre el objeto y el medio de registro, de manera que la distancia objeto-lente y lente-registro sean iguales a la distancia focal de la lente, como se muestra en la Figura 6. Esta lente convierte el plano del objeto y el plano del medio de registro en planos conjugados, realizando la transformada de Fourier entre ellos.

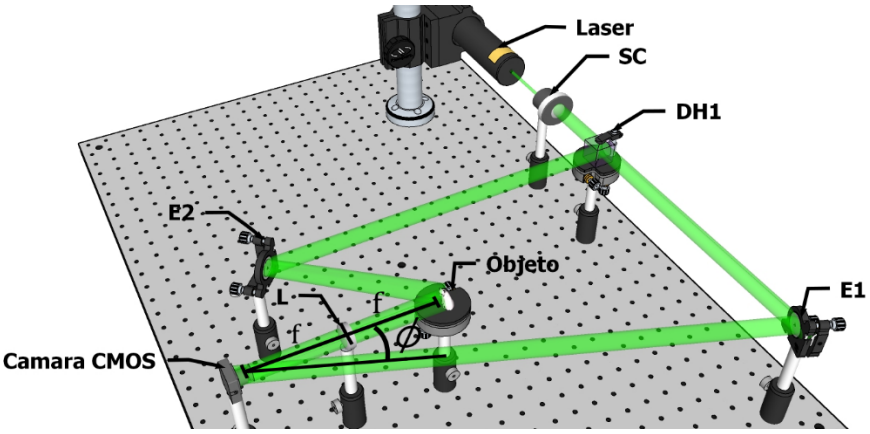

Figura 6: Esquema de un sistema de registro de hologramas de Fourier. SC: sistema de colimación, E: espejo, L: lente, f: distancia focal, DH: divisor de haz, ϕ : Angulo de la onda de referencia.

Esta configuración hace extremadamente simple la reconstrucción del holograma, ya que se puede llevar a cabo con una sola transformada rápida de Fourier, sin necesidad de especificar una distancia de reconstrucción. La forma del holograma de Fourier es similar a la de un holograma de Fresnel.

$$H(v,w) = |O(v,w)|^2 + |R(v,w)|^2 + O(v,w)R^*(v,w) + O^*(v,w)R(v,w) \tag{1.3.1}$$

Donde $O(v,w)$ es la transformada de Fourier de la luz dispersada por el objeto $o(x,y)$. Realizando la transformada de Fourier inversa, obtenemos

$$h(x,y) = o(x,y) \otimes o^*(x,y) + r^2 \; ro(x,y) \otimes \delta\left(x - \frac{x\sin\phi}{\lambda}\right) + ro^*(x,y) \otimes \delta\left(x + \frac{x\sin\phi}{\lambda}\right) \tag{1.3.2}$$

A diferencia de la transformada de Fresnel, la transformada de Fourier no presenta el factor cuadrático $\exp\left[-i\pi/\lambda d(k^2\Delta x^2 + l^2\Delta y^2)\right]$. Este factor hace que el complejo conjugado de una transformada de Fresnel sea igual a la misma transformada en la dirección contraria de propagación, es decir, que el complejo conjugado de una transformada de Fresnel a distancia d es igual a una transformada de Fresnel a distancia $-d$. En la práctica, esto significa que, a diferencia de los hologramas de Fresnel, en la reconstrucción de hologramas de Fourier no hay una imagen real y una virtual en lados opuestos del holograma, si no dos imágenes reales en el mismo plano, una del campo objeto y otra de su complejo conjugado, como se observa en la Figura 7.

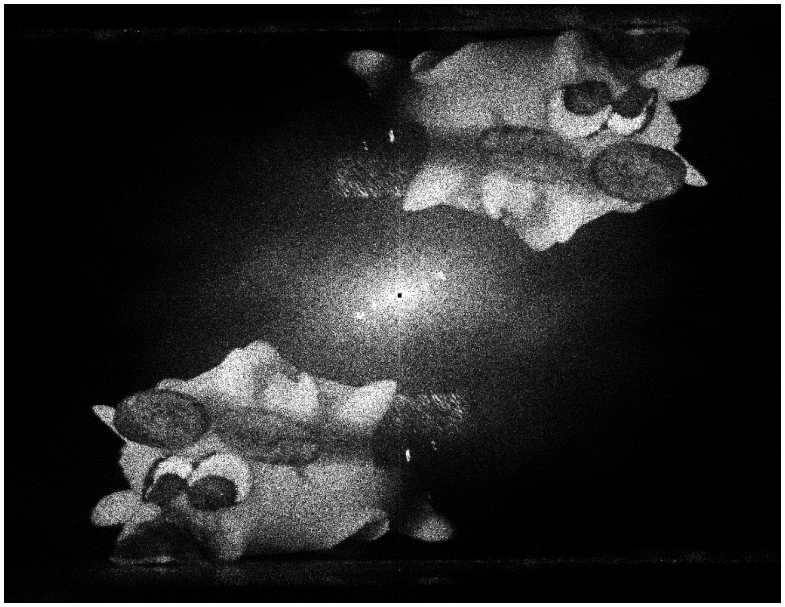

Figura 7: Reconstrucción de un holograma de Fourier.

La simplificación de la reconstrucción que se logra en los hologramas de Fourier tiene dos desventajas. La primera es que no es posible determinar un plano especifico de reconstrucción diferente al plano conjugado del holograma. Esto hace a la holografía de Fourier una opción poco deseable a la hora de registrar objetos 3D con profundidad extendida. Por otro lado, la introducción de una lente en el sistema óptico puede causar aberraciones que afecten la reconstrucción, y la pupila de la lente se convierte en una limitante adicional a la frecuencia espacial máxima del objeto. Estas características hacen a la holografía de Fourier una excelente opción cuando se desea registrar objetos 2D o 3D con poca profundidad.

1.4. Condiciones para el registro de hologramas.

Como se explicó anteriormente, un holograma es un diagrama de interferencia, y presenta franjas cuya frecuencia depende del ángulo entre la onda objeto y la onda de referencia. La frecuencia de las franjas del holograma debe ser menor que el tamaño de pixel del medio de registro. Esto no es un problema en las películas holográficas, debido al pequeño tamaño de las partículas fotosensibles que hacen el papel de pixel en las mismas, pero en las cámaras digitales, cuyos tamaños de pixel son mucho mayores, impone una seria limitación. La frecuencia máxima f_m que debe ser resuelta por el medio de registro se relaciona con el ángulo θ_m entre los haces así

$$f_m = \frac{2}{\lambda}\sin\theta_m \tag{1.4.1}$$

Y la frecuencia máxima que puede registrar una cámara digital con tamaño de pixel Δx es

$$f_m = \frac{1}{2\Delta x} \tag{1.4.2}$$

Otra restricción que debe tenerse en cuenta para el registro óptimo de hologramas tiene que ver con el rango dinámico del medio de registro. El rango dinámico se mide en decibelios (dB), y está dado por

$$DR = 10\log_{10}\left(\frac{I_{\max}}{I_{\min}}\right) \tag{1.4.3}$$

En el caso de películas holográficas o cámaras digitales, el rango dinámico es la relación entre la intensidad más alta $I_{\max}$ que puede registrar el medio correctamente y la más baja $I_{\min}$. La intensidad más alta es definida como aquella por encima de la cual la respuesta del medio deja de ser lineal. A este fenómeno se le conoce como saturación.

En una película holográfica, el rango dinámico típico ronda los 40-50 dB [8]. En una cámara digital moderna puede llegar a ser de 60 dB. En el registro de hologramas, el rango dinámico limita el tipo de objetos que se pueden registrar, debido a que la amplitud de las transformadas de Fourier y de Fresnel de un campo óptico pueden variar rápidamente de un punto a otro.

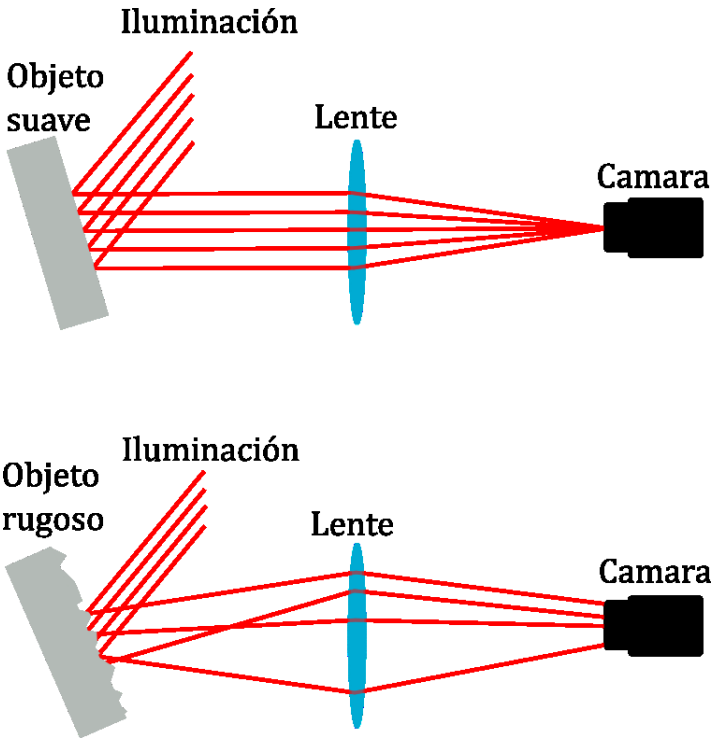

Figura 8: Efecto de la rugosidad de un objeto en la distribución de energía de su transformada de Fourier

En particular, la transformada de Fourier de un objeto con una superficie suave tiene un fuerte pico de intensidad en el centro del plano de Fourier y una concentración de la energía en un área pequeña. Este pico tiende a saturar el medio de registro, lo que implica perdida de información. Por otro lado, las transformadas de objetos con superficies rugosas tienen amplitudes con menores picos de intensidad y con una energía distribuida de manera más uniforme en el espacio. Esto implica que para registrar un objeto difuso es necesario mucho menos rango dinámico que para registrar un objeto suave o especular. Este efecto se ilustra en la Figura 8. Como se puede apreciar, los rayos provenientes de un objeto suave se propagan paralelos, y tras pasar por la lente convergen en el foco, mientras que los rayos del objeto difuso son dispersados en distintas direcciones, por lo que en el plano conjugado llegan a distintos puntos.

Una opción experimental usada para el registro óptico de hologramas de objetos suaves 2D con el propósito reducir el rango dinámico necesario, es ubicar un difusor (un vidrio rugoso) en contacto con la imagen u objeto. La rugosidad del vidrio se asemeja a una función de fase aleatoria, e idealmente cambia la fase de la luz que pasa por él sin alterar su amplitud, haciendo que la luz tome distintas trayectorias al llegar al medio de registro y así garantizando que la energía del campo este bien distribuida.

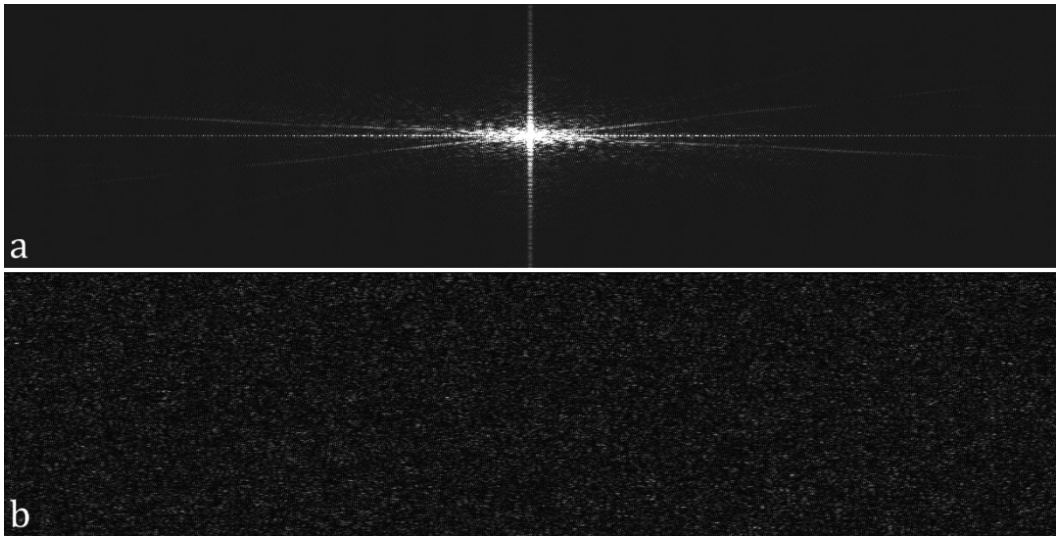

Figura 9: Hologramas de una imagen 2D a) holograma con registro directo, y b) holograma registrado con un difusor en contacto con la imagen.

Para ilustrar la diferencia en el rango dinámico requerido por un objeto suave y uno difuso, se registró el holograma de Fourier de una imagen 2D (Figura 9.a) y luego de la misma imagen multiplicada por una función de fase aleatoria (Figura 9.b), que simula el efecto de un difusor o pintura mate. Como se puede observar, el holograma de la imagen sin difusor presenta un fuerte pico en el centro, y de hecho su intensidad esta aumentada 10000 veces, pues de lo contrario solo se podría apreciar el pixel central. El rango dinámico de este holograma es de 89dB, lo que supera las capacidades de casi todas las películas holográficas o cámaras digitales. En el caso del holograma con difusor, su rango dinámico es de 54dB, el cual puede ser registrado cómodamente con películas y cámaras comerciales.

1.5. Filtrado.

Teniendo en cuenta las condiciones expuestas en la sección anterior, obtenemos que para una película holográfica con resolución de 5000 líneas/mm, el ángulo máximo entre los haces es de casi 180º, sin embargo, para la cámara CMOS usada para el registro de la Figura 4, es de tan solo 4.7º. Este ángulo limita el tamaño que puede tener el objeto registrado, especialmente si se desea evitar superposición entre el objeto y el orden cero tras la reconstrucción.

Debido a esta limitación, es importante reducir en la mayor medida posible el orden cero. Si revisamos el holograma $h(x,y)$ vemos que la expresión del orden cero es causada por las intensidades de la onda objeto y de la onda de referencia. Una forma simple de

reducir el mismo es registrar estas intensidades con el sistema experimental y restárselas al holograma. Esta técnica es de limitada utilidad, debido a que implica bloquear el haz objeto, registrar la onda de referencia, desbloquear el haz objeto y bloquear el haz de referencia para luego registrar la intensidad de la onda objeto. Además, es necesario garantizar que el sistema no sufra perturbaciones mecánicas durante el registro, que haría que las intensidades varíen respecto a las que se encuentran en el holograma. Todo este procedimiento hace más lento el registro de datos y dificulta las aplicaciones en tiempo real.

Es por estos motivos que es deseable reducir el orden cero sin registrar datos adicionales. Una forma de lograrlo es sustraer al holograma su promedio. Si reescribimos el holograma como

$$h(x,y) = o(x,y) + r + 2o(x,y)r\cos(\varphi_O - \varphi_R) \qquad (1.5.1)$$

Donde φ_O y φ_R son las fases de la onda objeto y la onda de referencia, y $o(x,y)$, r son sus amplitudes respectivamente, veremos que el tercer término, varía entre $\pm 2ro(x,y)$, por lo que su valor medio será 0. De esa manera, tras sustraer del holograma su promedio obtenemos

$$h(x,y) = o(x,y) - \overline{o(x,y)} + 2o(x,y)r\cos(\varphi_O - \varphi_R) \qquad (1.5.2)$$

Donde $\overline{o(x,y)}$ es el valor medio de $o(x,y)$. La resta $o(x,y) - \overline{o(x,y)}$ es en general menor que el orden cero original, logrando así la supresión de este en algunos casos, sin embargo, dependiendo de la extensión y rugosidad del objeto la reducción puede ser limitada, como se muestra en la Figura 10.

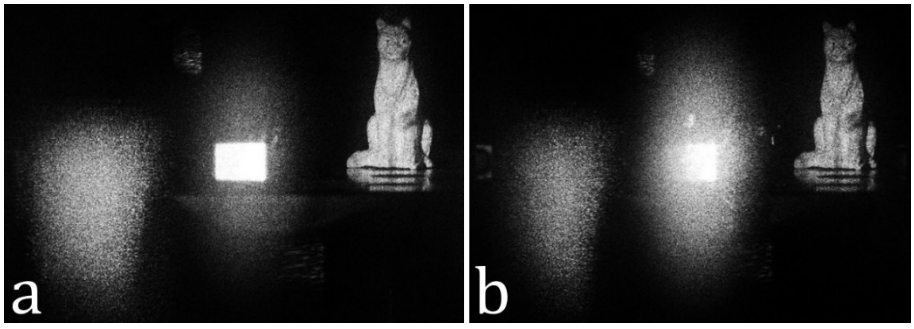

Figura 10: a) reconstrucción de un holograma sin supresión del orden central, b) reconstrucción con supresión del orden central sustrayendo el promedio del holograma.

Debido a que el desempeño de esta técnica depende de las características del objeto, es preferible recurrir a una técnica de filtrado digital para eliminar el orden central. Esta técnica de filtrado se lleva a cabo realizando la transformada de Fourier del holograma. Como se explicó anteriormente, los exponenciales que aparecen en la ecuación (1.2.4) producen una separación espacial de los términos del holograma, lo que se puede apreciar en la Figura 11. Gracias a esta separación, procedemos a multiplicar la transformada de Fourier del holograma por un filtro paso banda (Figura 11b), de forma que se elimina el orden central y la imagen virtual (Figura 11c). Realizando la transformada inversa de Fourier, finalmente obtenemos el campo objeto $o(x, y)$. Este campo se puede reconstruir usando la transformada de Fresnel, al igual que el holograma original, obteniendo así la imagen real del objeto, sin la imagen gemela ni el orden central, como se muestra en la Figura 11d.

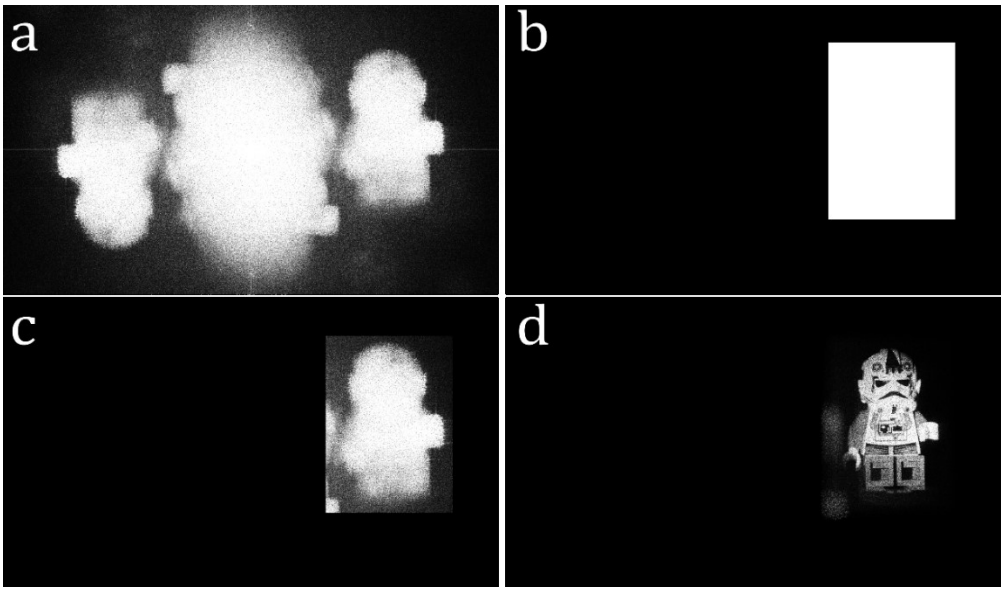

Figura 11: a) intensidad de la transformada de Fourier del holograma, b) filtro, c) transformada de Fourier del campo filtrado, d) reconstrucción del objeto a partir del campo óptico filtrado.

El filtrado digital de los hologramas es una técnica de gran utilidad, ya que elimina no solo el orden central si no también la imagen virtual, y permite aislar y extraer sólo la información correspondiente al campo óptico del objeto. Este campo ya no es un diagrama de interferencia, sino una función compleja cuya amplitud y fase se pueden manipular a voluntad. En el capítulo 3 de esta tesis, mostraremos que el filtrado es una forma de compresión sin perdida, pues permite reducir el volumen de datos del holograma sin afectar el campo óptico del objeto ni su reconstrucción.

1.6. Multiplexado.

Otra técnica digital de interés es el reposicionamiento del objeto. Si tomamos la transformada de Fourier del holograma filtrado, y recortamos el área que ocupa el objeto, podemos reposicionarlo digitalmente en cualquier lugar del espacio de reconstrucción. Esto matemáticamente equivale a convolucionar la transformada de Fourier del campo óptico con una delta de Dirac. Tras realizar la transformada de Fourier inversa, esta delta se convierte en un factor de fase que cambiara la posición de reconstrucción del objeto.

Este procedimiento es de gran utilidad a la hora de realizar multiplexado de hologramas. En general, multiplexar consiste en combinar varios canales o datos en uno solo, de manera reversible. Gran cantidad de sistemas usan técnicas de multiplexado, en especial cuando se desea aprovechar al máximo un canal de comunicación limitado, como un cable telefónico o de internet. Desde el punto de vista óptico, el concepto de multiplexado es similar al descrito, ya que tenemos un recurso limitado, como es el tamaño de nuestro medio de registro o la máxima frecuencia que puede resolver, y es deseable aprovecharlo al máximo.

En la referencia [9] mostramos la aplicación del multiplexado para superar el límite máximo del tamaño de una escena que se puede registrar con un sistema holográfico dado. Como se explicó en la sección anterior, la resolución y tamaño de pixel de la cámara determinan una frecuencia y tamaño máximo del objeto. Al tratar de registrar una escena que sobrepasa este límite, los distintos órdenes que componen la reconstrucción del holograma, es decir el orden cero, la imagen virtual y la imagen real, empiezan a superponerse, haciendo imposible la reconstrucción optima de toda la escena.

Figura 12: Registro de una escena de extensión superior al límite del sistema. A) Escena registrada, b) reconstrucción a partir de un holograma de Fresnel, c) reconstrucción a partir del campo óptico filtrado.

Como se aprecia en la Figura 12, cuando se registra una escena cuyas dimensiones superan las restricciones impuestas por el medio de registro, la reconstrucción de esta

no es óptima. En particular, sólo una parte de la escena es reconocible y está afectada por un elevado nivel de ruido. Debido a esto, no es posible registrar directamente una escena amplia por secciones. Esto se debe a que la luz proveniente de las secciones de la escena en las que no se cumplen los limites del medio de registro, introduce degradación en la reconstrucción del resto de la escena.

Así pues, si deseamos registrar una escena extendida, primero debemos iluminar sólo secciones que estén completamente dentro de los límites del sistema. Por ejemplo, la escena de la Figura 12 se puede registrar tomando hologramas por separado. Estos hologramas se pueden combinar para obtener el campo óptico de la escena completa por medio del multiplexado. El procedimiento es el siguiente:

Una vez se registra cada holograma, procedemos a filtrarlos. Tras multiplicar la transformada de Fourier del holograma por el filtro, podemos digitalmente reposicionar la región filtrada en cualquier lugar del espacio. De esta manera garantizamos que no haya superposición entre ellas. Tras este procedimiento, se obtienen los campos ópticos filtrados y reposicionados por medio de una transformada de Fourier inversa (TFI). Estos campos ópticos contienen la información del objeto y de su posición en el espacio, de manera que su suma corresponde a la escena completa.

Figura 13: Reconstrucción de una escena extendida obtenida a partir del multiplexado de tres hologramas.

La reconstrucción de la escena se lleva a cabo de forma igual a la de un holograma convencional. Como se muestra en la Figura 13, la escena así obtenida tiene una calidad muy superior a la obtenida sin multiplexado en la Figura 12.

El multiplexado no está limitado al ensamble de escenas en un solo plano. En el caso de hologramas de Fresnel, los planos de reconstrucción de cada objeto pueden ser diferentes, permitiendo así la construcción de escenas con una profundidad mayor a la de los objetos que la componen.

Cuando deseamos crear escenas con profundidad a partir de hologramas registrados con las mismas distancias objeto-cámara, podemos cambiar digitalmente el plano de reconstrucción de un objeto usando una lente virtual.

Recordemos que la fase de una lente esta descrita por la función

$$L = \exp\left[i\frac{\pi}{\lambda f}\left(x^2 + y^2\right)\right] \tag{1.6.1}$$

Si multiplicamos el holograma por una lente, y aplicamos la transformada de Fresnel, tenemos que

$$\begin{aligned}\Gamma(\eta,\xi) &= \frac{i}{\lambda d}\exp\left(-i\frac{2\pi}{\lambda}d\right)\exp\left(-i\frac{\pi}{\lambda d}(\eta^2+\xi^2)\right)\\ &\int_{-\infty}^{\infty}\int_{-\infty}^{\infty} R(x,y)h(x,y)L(x,y)\exp\left[-i\frac{\pi}{\lambda d}(x^2+y^2)\right]\\ &\exp\left[i\frac{2\pi}{\lambda d}(x\eta+y\xi)\right]dxdy\\ &= \frac{i}{\lambda d}\exp\left(-i\frac{2\pi}{\lambda}d\right)\exp\left(-i\frac{\pi}{\lambda d}(\eta^2+\xi^2)\right)\\ &\int_{-\infty}^{\infty}\int_{-\infty}^{\infty} R(x,y)h(x,y)\exp\left[-i\frac{\pi}{\lambda}\left(\frac{1}{d}-\frac{1}{f}\right)(x^2+y^2)\right]\\ &\exp\left[i\frac{2\pi}{\lambda d}(x\eta+y\xi)\right]dxdy\end{aligned} \tag{1.6.2}$$

Como se observa en la ecuación anterior, el factor exponencial de la lente cambia la distancia efectiva de la transformada de Fresnel, pasando de d a $\left(\frac{df}{f-d}\right)$, cambiando el plano de reconstrucción. El nuevo plano de reconstrucción sería entonces $\left(\frac{1}{d}+\frac{1}{f}\right)$.

Con la combinación del filtrado, reposicionado y el uso de lentes virtuales, es posible alterar a voluntad la posición tridimensional de un objeto registrado por medio de holografía digital. Esto permite, con el uso de técnicas de multiplexado, generar escenas

considerablemente más complejas que las que posibles con un sistema de holografía dado.

1.7. Holografía digital a color.

En la descripción que hemos hecho hasta ahora de la holografía digital, no hemos tratado el registro de la información del color. El registro de esta información aumenta considerablemente la complejidad y costo de los sistemas holográficos, y en la practica la información cromática de los objetos no es necesaria para gran parte de las aplicaciones de la holografía, sin embargo, hay aplicaciones donde es imprescindible. Por ejemplo, en la microscopia holográfica, el registro del color es necesario para diferenciar partes de una célula. En aplicaciones donde se desea una reconstrucción lo más fiel posible del objeto, como un display holográfico, el color es necesario.

Los hologramas mostrados en las secciones anteriores fueron registrados con una fuente laser la cual produce luz cuasi monocromática. Esta luz ilumina el objeto, es dispersada por el mismo y luego de propagarse llega al sensor. Esta dispersión dependerá no solo de las características de la superficie del objeto, si no de su reflectancia en la longitud de onda de iluminación. Así pues, con excepción de objetos que tienen igual reflectancia en todo el espectro, el mismo holograma del mismo objeto tomado con diferentes colores puede tener información diferente. De esta manera, el campo objeto se convierte en una función de la longitud de onda.

Si quisiéramos recuperar la información completa del objeto, sería necesario iluminarlo con luz blanca que contenga todas las longitudes de onda, y registrar el holograma resultante

$$h(x,y)=\int_{380}^{700}|O(x,y,\lambda)|^2+|R(x,y,\lambda)|^2 \\ +O(x,y,\lambda)R^*(x,y,\lambda)+O^*(x,y,\lambda)R(x,y,\lambda)d\lambda \tag{1.6.3}$$

En la práctica no es posible registrar hologramas con todas las longitudes de onda simultáneamente, ya que las fuentes de gran ancho de banda espectral son en general incoherentes. Esta dificultad fue evidente desde el principio de la holografía, y las primeras estrategias para superarla fueron planteadas en el trabajo seminal de Leith & Upatnieks [10]. En este trabajo, se proponía reconstruir el objeto a color a partir de tres hologramas registrados con tres longitudes de onda, correspondientes al color rojo,

verde y azul. La superposición incoherente de los objetos reconstruidos a partir de estos tres hologramas sería el objeto a color.

La mayoría de los sistemas de holografía a color usa esta propuesta, sin embargo, vale la pena señalar que la reproducción a color lograda de esta manera no es sino una aproximación al objeto real.

Para entender el porqué de esta inexactitud, basta con asumir que cada holograma de cada longitud de onda equivale a una medida del muestreo del campo óptico del objeto, que es una función de la longitud de onda. Con solo tres longitudes de onda, el muestreo de esta función puede sufrir de aliasing [11], haciendo que dos colores distintos se reproduzcan como el mismo. Como en el muestreo de cualquier función, la reproducción de la misma mejora cuando se aumenta el número de muestras, no obstante, tomar una muestra adicional de la información a color requiere una nueva fuente de iluminación en la longitud de onda correspondiente, lo que aumenta significativamente la complejidad del sistema de registro. Afortunadamente, la reflectancia de la mayoría de los objetos varia de forma relativamente suave con la longitud de onda, haciendo posible una reconstrucción aceptable del color con pocas fuentes. En particular, el número óptimo de longitudes de onda es 4, y más de 7 no produce una reducción importante en el error en la reconstrucción de color [11].

1.7.1. El espacio de color.

La elección de las longitudes de onda para el muestreo de la información a color también es importante, ya que determina que colores son posible registrar adecuadamente por el sistema o el espacio de color de este. Existen diversas formas de representar los espacios de color, sin embargo, para la holografía digital, que usa fuentes casi monocromáticas, el diagrama de la Comisión Internacional de Color (CIE) es tal vez el de más utilidad.

Este diagrama es una representación bidimensional donde cada color tiene asignado unas coordenadas (x, y). Estas coordenadas dependen de valores de triestimulo del ojo de un observador promedio. El triestimulo es la respuesta al estímulo de cada uno de los tres tipos de cono (células sensibles a la longitud de onda) en el ojo humano. Para colores observados por reflexión, estos valores son dados por

$$X = \int_{\lambda} S(\lambda) I(\lambda) \tilde{}$$
$$Y = \int_{\lambda} S(\lambda) I(\lambda) \tilde{} \qquad (1.6.4)$$
$$Z = \int_{\lambda} S(\lambda) I(\lambda) \tilde{}$$

Donde $S(\lambda)$ e $I(\lambda)$ son la reflectancia del objeto y la intensidad de la fuente respectivamente, las cuales son funciones de la longitud de onda y $\tilde{}$, $\tilde{}$ y $\tilde{}$ son las respuestas cromáticas de un observador ideal. Con las funciones de triestimulo de la ecuación (1.6.4) se construye el diagrama de color, definiendo los ejes coordenados como

$$x = \frac{X}{X+Y+Z};$$
$$y = \frac{Y}{X+Y+Z}; \qquad (1.6.5)$$
$$z = 1 - x - y;$$

En el caso de la holografía a color, las fuentes luminosas corresponden a láseres, cuya luz es casi monocromática. En la representación CIE, los colores puros espectralmente limitan una figura con forma de herradura o lengua (de ahí la expresión “lengua de color”), cuyo interior contiene todos los colores perceptibles por el ojo humano. Para un sistema dado, el espacio de color de este sería el área de un polígono cuyos vértices corresponden a los colores de las fuentes de iluminación usadas.

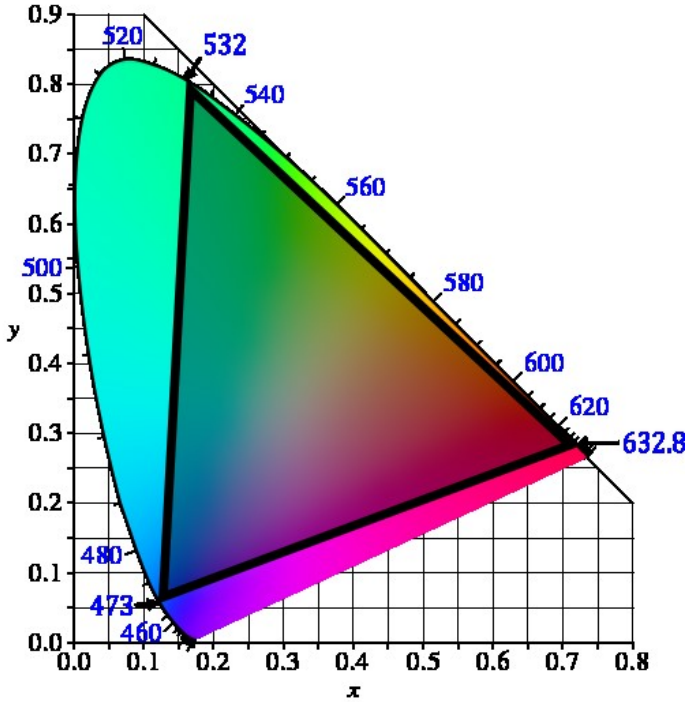

Figura 14: Espacio de color para 3 fuentes cuasi monocromáticas de 473 nm, 532 nm y 632.8 nm.

En la Figura 14 se muestra el diagrama de color CIE, con el espacio de color disponible para un sistema holográfico de 3 fuentes laser con longitudes de onda 473 nm, 532 nm y 632.8 nm, dado por el área sombreada. Esta representación del espacio de color permite elegir el número y las longitudes de onda de las fuentes para maximizar el espacio de color disponible. En la práctica, sin embargo, algunos láseres presentan más bajo costo y mayor eficiencia que otros, lo cual también debe tenerse en cuenta para construir sistemas de holografía a color.

1.7.2. Registro de hologramas a color.

En la Figura 15 se muestra un sistema para el registro de hologramas a color con tres fuentes laser. Los colores de objetos reconstruidos a partir de los hologramas registrados con este sistema están en el espacio de color de la Figura 14.

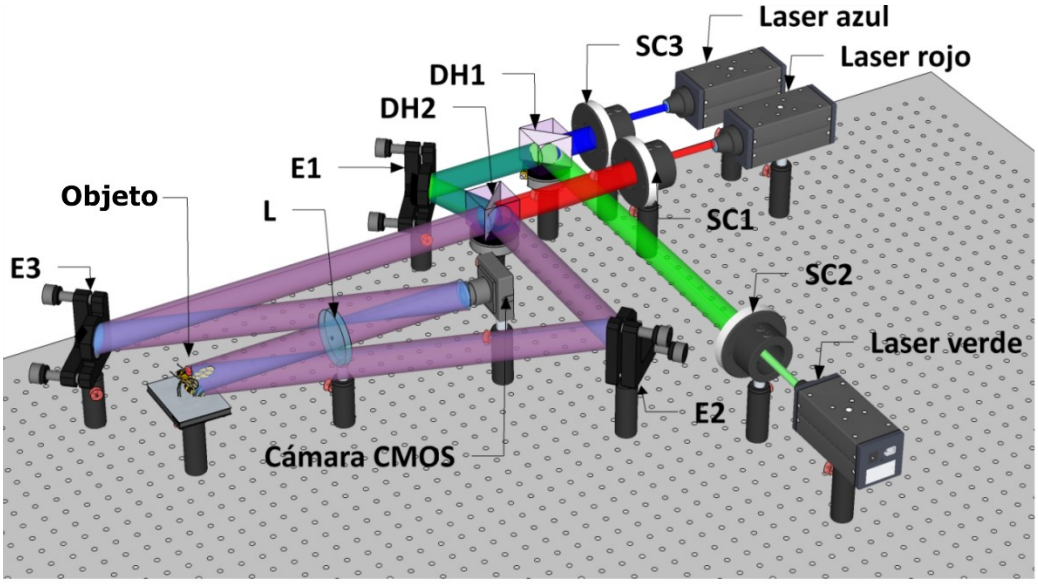

Figura 15: Sistema de registro de hologramas de Fourier a color (DH: divisor de haz, SC: sistema de colimación, E: espejo, L: lente)

Los hologramas del objeto pueden registrarse individualmente, iluminando el mismo con cada longitud de onda y registrando los tres hologramas uno tras otro, o si se dispone de una cámara a color, en un solo registro, iluminando el objeto con las tres longitudes de onda simultáneamente.

Si se usa una cámara a color se debe tener en cuenta que estas cámaras utilizan un filtro Bayer. El filtro Bayer es un filtro con una estructura de tablero de ajedrez ubicado

antes del sensor de la cámara, como se muestra en la Figura 16, el cual hace que en cada grupo de cuatro pixeles haya dos que solo son sensibles al verde, uno al rojo y otro al azul.

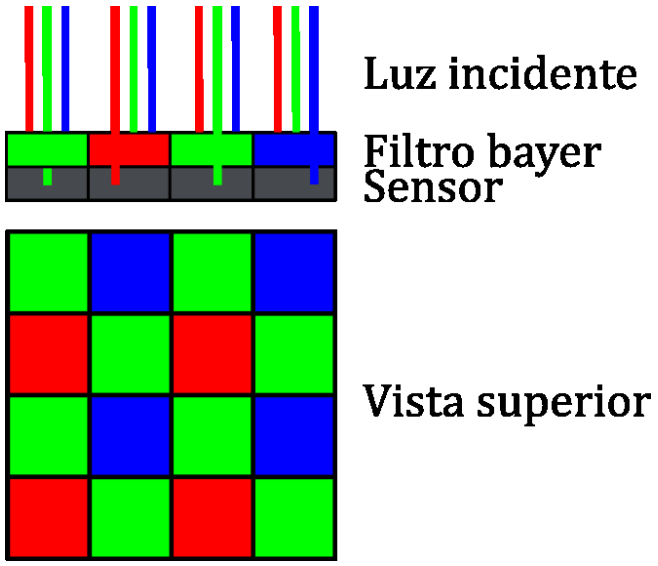

Figura 16: Esquema del filtro Bayer en una cámara a color.

Esto significa que la resolución efectiva de los hologramas tomados con cámaras a color será la mitad de la resolución total para el verde y un cuarto para el rojo y el azul. Las cámaras a color usan un algoritmo para combinar los valores de intensidad de los grupos de cuatro pixeles para asignarle valores en color rojo, verde y azul (RGB) a todo el bloque de cuatro pixeles. En el caso del registro de hologramas, este algoritmo produce superposición entre los canales, por lo que es preferible tomar los datos en el formato bruto (RAW), el cual guarda la intensidad registrada por cada pixel sin ningún postprocesado. Luego se usan mascaras con el patrón Bayer para extraer de esa imagen RAW los hologramas de cada canal de color, como se muestra en la Figura 17.

Además de los efectos del filtro Bayer cuando se realiza el registro holográfico de una sola toma con cámaras a color, también debe tenerse en cuenta que la frecuencia de las franjas de interferencia entre el campo objeto y el haz de referencia depende de la longitud de onda. Como explicamos en la sección 1.2, la frecuencia de las franjas de interferencia está dada por $sen(\theta)/\lambda$, donde θ es el ángulo entre la onda objeto y la onda de referencia y λ es la longitud de onda.

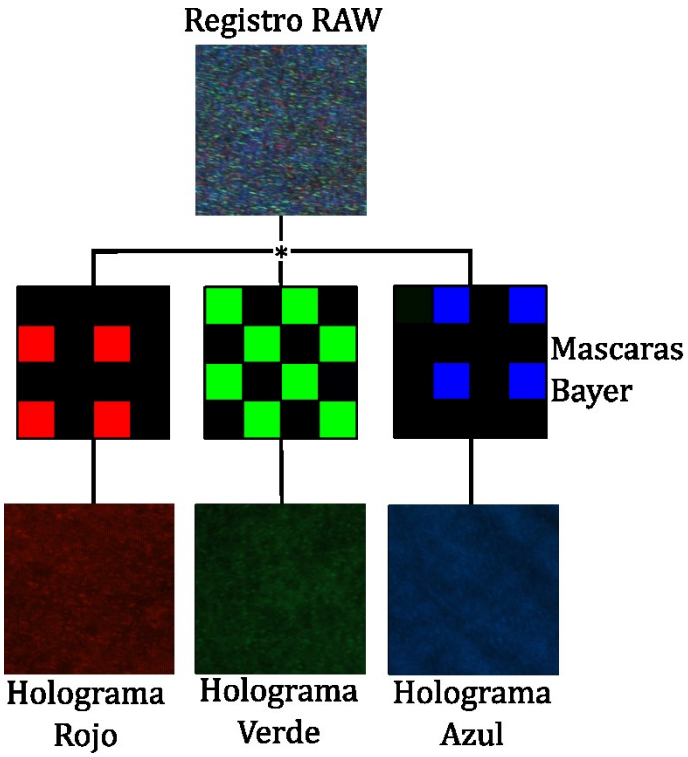

Figura 17: Registro holográfico a color en un solo paso.

Esta dependencia de la longitud de onda implica que, si se usa el mismo ángulo para todas las fuentes laser, las franjas de interferencia de las longitudes de onda mayores tendrán menor frecuencia. Este efecto se traduce en diferentes separaciones entre el orden central y el objeto reconstruido para cada canal, y puede hacer que para algunas longitudes de onda la frecuencia de las franjas supere la condición de muestreo. Existen dos opciones para corregir este defecto. La primera es simplemente usar diferentes ángulos de incidencia para cada longitud de onda, de manera que se garantice la misma frecuencia f de las franjas para todas las longitudes de onda. Así

$$\theta = sen^{-1}\left(f\lambda\right) \tag{1.6.6}$$

Esta opción es impráctica, debido a que un cambio en la longitud de onda produce cambios pequeños del ángulo (del orden de minutos de arco) que son difíciles de lograr experimentalmente. Adicionalmente, para guiar cada onda de referencia se requieren espejos y elementos ópticos adicionales.

La otra opción consiste en usar el mismo ángulo para todas las fuentes, como en la Figura 15. En este caso, se debe garantizar que el ángulo escogido cumpla la condición de muestreo para la longitud de onda más baja usada en el sistema, y a su vez que $sen(\theta)/\lambda$

sea lo suficientemente grande para evitar la superposición entre el objeto reconstruido y el orden central para la longitud de onda más alta. Así

$$sen^{-1}\left(f_{\min}\lambda_{\max}\right) < \theta < sen^{-1}\left(f_{\max}\lambda_{\min}\right) \qquad (1.6.7)$$

donde $f_{\min}$ es la frecuencia mínima de las franjas necesaria para evitar superposición entre el objeto reconstruido y el orden central y $f_{\max}$ es la máxima frecuencia que se puede registrar con nuestra cámara. La diferencia en la posición de reconstrucción de cada canal luego es corregida por medio de un reposicionado digital, como se explicó en la sección 1.5.

1.7.3. Reconstrucción de hologramas a color.

La reconstrucción digital de hologramas a color se lleva a cabo de la misma manera que la de hologramas convencionales. Cada canal es reconstruido individualmente, y luego se superponen las reconstrucciones resultantes, asignándole a cada una el color apropiado según la fuente empleada para su registro. Este proceso tiene algunas dificultades que deben tenerse en cuenta. La primera de ellas es la producida por la dependencia de la frecuencia de las franjas de los hologramas con la longitud de onda, la cual se puede resolver por medio del reposicionado digital o eligiendo los ángulos de incidencia de la onda de referencia, como se explicó anteriormente.

La segunda dificultad radica en que la longitud de onda tiene efectos en la reconstrucción digital de los hologramas, tanto cuando son de Fresnel como de Fourier. En la discusión de la transformada de Fresnel en la sección 1.2., realizamos el siguiente cambio de variable

$$v = \frac{\eta}{\lambda d}; \quad \mu = \frac{\xi}{\lambda d} \qquad (1.6.8)$$

Y adicionalmente, mostramos que el tamaño de pixel en (v, μ) esta relacionado con el tamaño de pixel de la cámara por

$$\Delta v = \frac{1}{M\Delta x}; \qquad \Delta\mu = \frac{1}{N\Delta y} \qquad (1.6.9)$$

Combinando (1.6.8) y (1.6.9), obtenemos los tamaños de pixel en el plano de reconstrucción, dados por

$$\Delta\eta = \frac{\lambda d}{M\Delta x}; \quad \Delta\xi = \frac{\lambda d}{N\Delta y} \tag{1.6.10}$$

De las relaciones anteriores, encontramos que el tamaño de pixel en el plano de reconstrucción dependerá tanto de la longitud de onda como de la distancia de propagación. Esta dependencia causa un cambio de escala en los objetos reconstruidos, lo que dificulta la superposición de los canales de color. Adicionalmente, para algunas aplicaciones, es conveniente mantener el tamaño de reconstrucción fija con hologramas tomados con distintas distancias, por ejemplo, cuando se quiere realizar seguimiento de muestras en tres dimensiones usando microscopia holográfica. Ferraro et al [12] mostraron que, para que el tamaño de pixel en el plano de reconstrucción de dos hologramas registrados con longitudes de onda diferentes sea igual, se debe cumplir que

$$M_2 = \frac{M_1\lambda_2}{\lambda_1}; \quad N_2 = \frac{N_1\lambda_2}{\lambda_1} \tag{1.6.11}$$

Donde $M_1 \times N_1$ es el número de pixeles del holograma registrado con longitud de onda λ_1 y $M_2 \times N_2$ el del holograma registrado con λ_2. Disminuir el número de pixeles de un holograma para cumplir la condición anterior implica perdida de datos, pero un aumento puede lograrse sin afectar la calidad de la reconstrucción, simplemente añadiendo pixeles negros alrededor del holograma. Debido a esto, se deja sin alterar el holograma con menor longitud de onda, y se añade ceros a todos los demás.

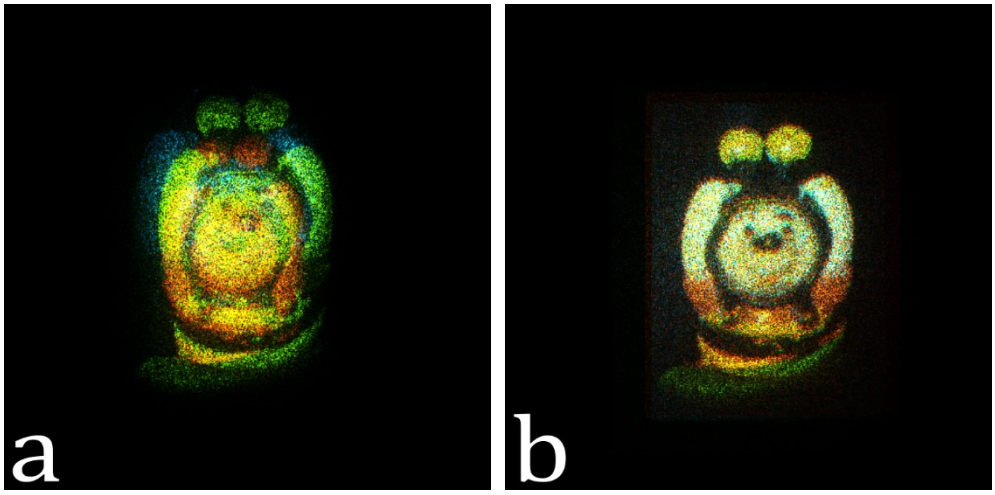

Figura 18: Objeto a color reconstruido con hologramas de tres longitudes de onda. A) sin corrección de escala, b) con corrección de escala.

En la Figura 18 se muestra la reconstrucción de un holograma a color sin corrección de escala y con ella. Estos resultados fueron obtenidos usando el esquema de la Figura

15. El medio de registro fue una cámara CMOS a color de 3840x2720 pixeles de resolución, con un tamaño de pixel de 1.6 μm. Los tres hologramas se obtuvieron secuencialmente. Se usaron fuentes laser de 473 nm, 532 nm y 632.8 nm con potencia de 50, 150 y 75 mW respectivamente. El ángulo de incidencia de los haces de referencia fue de 4.8° para todas las longitudes de onda. Se filtraron los hologramas restando el promedio de su intensidad y se utilizó reposicionado digital para garantizar la superposición de los canales después de la corrección de escala.

1.8. Hologramas de fase pura

Como ultimo tópico en este capítulo, trataremos un tipo particular de hologramas, que son aquellos donde la información del objeto está contenida completamente en la fase, es decir, que la amplitud del campo óptico registrada en el plano del holograma es casi uniforme. Este tipo de hologramas son de especial interés, ya que su procesado y almacenamiento se simplifica notablemente, pues la información de amplitud puede descartarse. Adicionalmente, estos hologramas pueden registrarse sin necesidad de medios con un alto rango dinámico, ya que la variación de su intensidad es mínima.

Finalmente, debido a que no existen actualmente dispositivos capaces de modular simultáneamente la amplitud y la fase de un campo óptico, los hologramas de fase pura permiten controlar el campo óptico de forma efectiva usando sólo cambios de fase, haciendo posible así la construcción de displays holográficos.

Desde los años sesenta, cuando la investigación en análisis espectral de señales presentó enormes avances, se observó que la información de fase de las transformadas de Fourier o Fresnel de una señal tiene mayor importancia que su amplitud a la hora de reconstruirla. Esto se debe a que la fase contiene la información sobre la ubicación espacial de las características de la misma (en el caso de que la señal sea una imagen) [13].

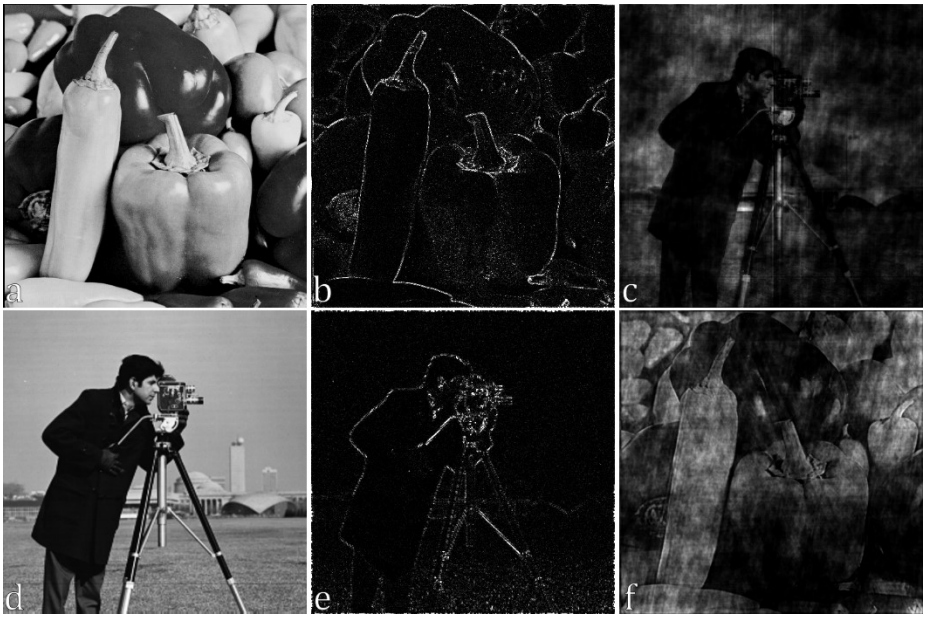

Figura 19: Ejemplo de la importancia de la fase de la TF de una señal. a) y d) objetos originales. b) y e) imágenes reconstruidas a partir de la fase de la TF de a) y d). c) y f) imágenes reconstruidas intercambiando las fases de las TFs de a) y d).

En la Figura 19 se demuestra la importancia de la fase para la reconstrucción de una señal a partir de su TF. Para esto, se realizó la transformada de Fourier de dos imágenes (Figura 19.a y d). Luego, se hizo la amplitud de estas TFs igual a la unidad y se aplica la TFI al resultado, obteniendo las imágenes de la Figura 19.b y e. En este resultado se aprecia como la reconstrucción a partir de solo la información de fase da énfasis a los bordes de la imagen, pero mantiene la estructura general de la misma. Por último, se intercambió la fase de las TFs de las imágenes de entrada, manteniendo la amplitud. Tras realizar la TFI del resultado, se obtiene las imágenes de la Figura 19.c y f, las cuales tienen el contenido correspondiente a la fase, no a la amplitud.

Ahora bien, si la fase contiene el grueso de la información de una imagen o señal, ¿qué características debe tener esta señal para que la reconstrucción a partir de su fase sea lo más cercana al objeto original? La fase de la TF de una señal contiene la información de la estructura espacial de la misma, mientras que la amplitud tiene la información sobre cuanta energía corresponde a cada característica de la señal. Es por esto que al hacer la amplitud de las TF de la Figura 19 igual a la unidad las imágenes reconstruidas tienen mayor intensidad en los bordes, ya que estos corresponden a frecuencias altas en la TF. Por otro lado, las frecuencias bajas, correspondientes a las zonas de la imagen con poco cambio de intensidad, y tienen una amplitud muy alta. Al hacer unidad la amplitud de la TF, se está entonces reduciendo la amplitud de las frecuencias bajas y aumentando la de

las altas, dando lugar al resultado de la Figura 19.b y e. Teniendo en cuenta lo anterior, podemos suponer que una imagen, cuya TF tenga amplitud uniforme o con pocas variaciones, se podrá reconstruir a partir de la información de fase con mayor fidelidad.

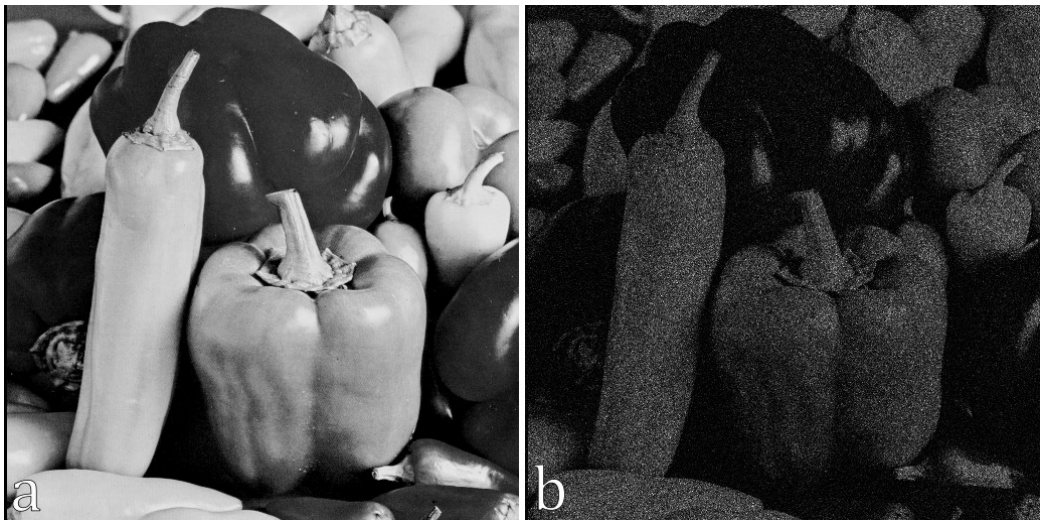

Figura 20: Reconstrucción de una imagen a partir de la fase de la TF de su producto con un difusor. a) imagen original, b) reconstrucción.

Una forma de verificar esta suposición es tratar de reconstruir una imagen a partir de la fase de la TF de su producto con una máscara de fase aleatoria. Como se explicó en la sección 1.4, una máscara de fase tiene el efecto de distribuir la energía de la TF de un objeto. En la Figura 20 se muestra el resultado de esta prueba. Como esperábamos, la imagen reconstruida ya no presenta énfasis en los bordes, y aunque está afectada por speckle, se asemeja mucho más a la imagen original que el resultado de la Figura 19. De esta manera, podemos concluir que los objetos difusos se pueden reconstruir aproximadamente con la información de fase de sus transformadas de Fourier. La transformada de Fresnel presenta un comportamiento análogo, en tanto hereda las propiedades básicas de la transformada de Fresnel.

Como un holograma contiene la información de las transformadas de Fourier o de Fresnel del campo óptico del objeto, el comportamiento de estos será análogo al de los resultados de la Figura 19. De esta manera, mientras el objeto sea difuso, se puede lograr una reconstrucción aproximada a partir de la fase del campo extraída del holograma [14].

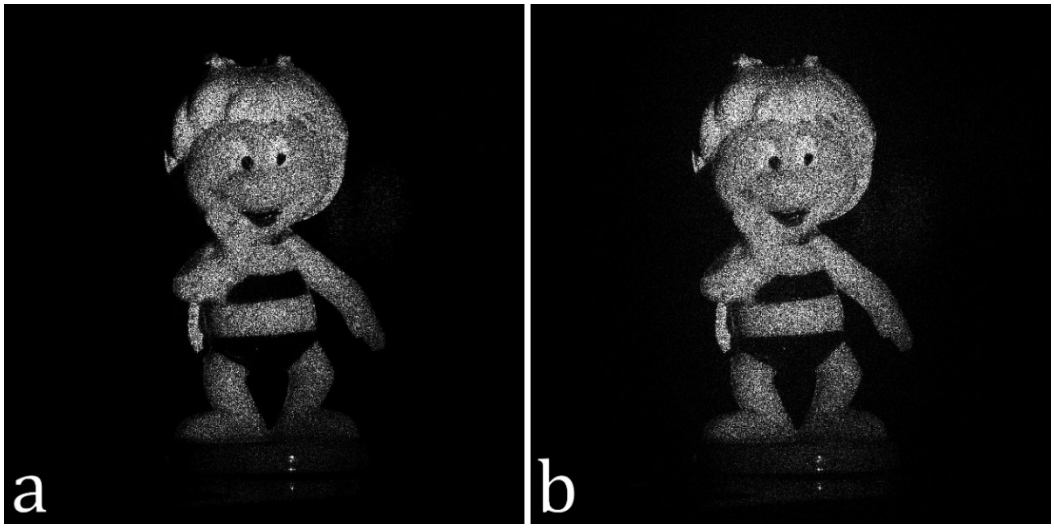

Figura 21: Reconstrucción de un holograma de Fresnel de un objeto difuso. a) reconstrucción con el campo óptico complejo, b) reconstrucción con solo la fase.

En la Figura 21 se muestra este efecto. Para ello, se registró un holograma de Fresnel de un objeto difuso usando el esquema de la sección 1.2. Tras filtrar el holograma, se realizó la reconstrucción del objeto de la forma usual, obteniendo el resultado de la Figura 21.a. Para obtener el resultado de la Figura 21.b, usando el mismo holograma, se hace la amplitud del campo resultante del filtrado igual a la unidad y se realiza la TFrI necesaria para la reconstrucción. Como se puede apreciar, la diferencia entre ambos resultados es casi imperceptible. Hay un leve aumento del ruido de speckle alrededor de las zonas brillantes de la imagen, pero la reconstrucción no se ve fuertemente afectada.

De esta manera, demostramos que solo la información de fase del campo óptico es suficiente para reconstruir satisfactoriamente un objeto difuso. Esta característica tiene importantes consecuencias para la compresión y visualización de datos holográficos, las cuales discutiremos en los capítulos III y IV.

II. Encriptación con holografía digital

2.1 Introducción.

Los últimos años del siglo XX y lo que va del siglo XXI han sido testigos de una verdadera revolución en el área de las telecomunicaciones, gracias al desarrollo del internet, las redes satelitales y la fibra óptica, entre otros muchos avances científicos y tecnológicos. Gracias a esta revolución, nunca ha sido más fácil y económico enviar y recibir grandes cantidades de datos, y los gobiernos, empresas, sistemas financieros y redes sociales se han desarrollado para tomar ventaja de estas capacidades.

Paralelamente al crecimiento en el flujo de datos en las sociedades modernas, nos encontramos con el apremiante reto de garantizar la privacidad y seguridad de los mismos. Aunque la seguridad de los datos es un problema multidimensional en el cual se deben tener en cuenta desde la arquitectura misma de las redes de comunicación hasta la confiabilidad de los usuarios, una de las facetas más antiguas y estudiadas de la misma es la criptografía. La palabra criptografía deriva de las palabras griegas “kryptos” cuya traducción aproximada es “secreto” y “graphein” que significa “escribir”. Así pues, la criptografía estudia como “escribir en secreto” o “esconder la escritura”. En la práctica, la criptografía es el estudio y desarrollo de técnicas para comunicación segura en presencia de terceros, denominados adversarios, que buscan acceder a los datos protegidos. Una de las ramas más importantes de la criptografía es la encriptación, la cual consiste en técnicas por medio de las cuales una información es codificada en una nueva representación que sea incomprensible para un adversario. Este proceso luego puede revertirse si se dispone de una determinada llave de seguridad, que poseerán los usuarios autorizados.

Los primeros ejemplos de encriptación datan del año 1900 A.C, y consistían en cifrados por sustitución, en los cuales los caracteres de un idioma eran reemplazados uno a uno por otro set de caracteres. Otro tipo de encriptación clásica es el cifrado por transposición, donde las letras de un mensaje eran reordenadas siguiendo cierta regla. Durante la mayor parte de la historia de la humanidad, este tipo de cifrado por sustitución y transposición fue el estado del arte de la encriptación, sin embargo, en los últimos años del siglo XIX Claude Shannon estableció los principios de la teoría de la información, dando pie a la formalización de la criptografía como área de estudio y a los primeros avances en criptografía teórica.

Ya en el siglo XX, las necesidades bélicas de las grandes guerras junto con el desarrollo de las primeras computadoras, tanto mecánicas como electrónicas, resulto en un gran avance del campo, con el desarrollo de múltiples algoritmos de encriptación (como por ejemplo la infame maquina Enigma de las fuerzas alemanas en la segunda guerra mundial). A su vez, comenzó a ser de gran interés el criptoanálisis, es decir, el estudio de las vulnerabilidades de las técnicas de encriptación.

Con el gran poder de computo disponible actualmente las técnicas de criptoanálisis se han vuelto más sofisticadas, siendo necesario el desarrollo de nuevos algoritmos de encriptación para mantener la seguridad. Debido a las demandas de esta competencia, el estudio de nuevas alternativas para lograr la encriptación es de gran interés.

Es en este panorama que se comenzaron a estudiar las posibilidades que ofrecían los sistemas ópticos para la encriptación de datos. Los sistemas ópticos tienen la ventaja de ser inherentemente paralelos, en teoría pueden procesar datos a la velocidad de la luz, y presentan múltiples grados de libertad que pueden ser de utilidad para diseñar distintos métodos de encriptación, como la fase, la polarización, el momento angular, entre otros. La primera aproximación al concepto de encriptación óptica fue realizada en 1976 [15], sin embargo, no fue sino hasta el trabajo seminal de Refrieger & Javidi [16] que se comenzó a estudiar la encriptación óptica con implementaciones experimentales. Este tipo de encriptación óptica es denominado encriptación de doble fase aleatoria (DRPE por las siglas en ingles de double random phase encryption), debido a que usa la convolución de dos funciones aleatorias de fase para convertir el dato encriptado en un diagrama de ruido blanco.

De los múltiples esquemas DRPE presentes en la literatura, sobresalen el 4f, que fue el sistema original propuesto por Refrieger y Javidi y el primero en ser demostrado experimentalmente [17], y el criptosistema de correlador de transformada conjunta (JTC por las siglas en ingles de joint transform correlator) [18]. Este último esquema es de especial interés debido a que la información encriptada en el mismo es la intensidad de la interferencia entre dos funciones. Esta intensidad puede ser registrada por una cámara digital, haciendo posible la implementación de sistemas híbridos opto-digitales, que combinan las ventajas de las técnicas ópticas con la flexibilidad de los sistemas digitales.

Al igual que los sistemas de holografía, los sistemas DRPE pueden ser implementados usando distintas transformaciones entre el plano de entrada y el plano de salida, como lo es la transformada de Fourier, la de Fourier fraccionaria y la de Fresnel.

A pesar de que los sistemas ópticos de encriptación ofrecen un gran potencial para la protección de datos, también tienen desventajas. La primera de estas desventajas es que el criptoanálisis de los sistemas ópticos ha demostrado algunas vulnerabilidades de la implementación original de DRPE. Al igual que con los sistemas tradicionales de encriptación, el descubrimiento de estas vulnerabilidades ha resultado en modificaciones a los sistemas para hacerlos más seguros. A pesar de estos esfuerzos, el criptoanálisis de los sistemas ópticos no ha alcanzado el mismo grado de desarrollo que en los sistemas tradicionales, lo que hace difícil analizar la seguridad de estas modificaciones.

La otra desventaja consiste en la aparición de ruido en los datos desencriptados. Este ruido se manifiesta como speckle que afecta el objeto recuperado, e inclusive puede llegar a hacerlo irreconocible. Esta degradación limita el volumen y complejidad de los datos que pueden encriptarse en un sistema dado. Diversas propuestas han intentado evitar esta limitación de los sistemas ópticos, por ejemplo, introduciendo la información a ser encriptada en un "contenedor" cuyas características lo hacen más resistente a la degradación durante el proceso de encriptación. De esta manera, tras desencriptar, el contenedor presenta ruido, pero la información que contiene puede extraerse sin afectación.

En este capítulo mostraremos como los sistemas DRPE están estrechamente relacionados con la holografía, se implementará experimentalmente un criptosistema JTC tradicional, con transformada de Fourier fraccionaria y transformada de Fresnel. Estudiaremos algunas de las vulnerabilidades de los sistemas DRPE y se implementara

una técnica novedosa para hacer el sistema más seguro. Luego se estudiará el problema del ruido en los sistemas DRPE y demostraremos varias técnicas para reducirlo. También discutiremos el concepto de contenedor de la información, incluyendo un diseño que tiene en cuenta las propiedades de los sistemas DRPE. Finalmente, se demostrara la encriptación de objetos 3D usando llaves volumétricas.

2.2. Principios de la encriptación con doble mascara de fase

El desarrollo de la encriptación óptica tiene sus inicios en el estudio de los denominados correladores ópticos. Un correlador es un sistema que permite realizar la operación de correlación entre dos funciones. Realizar esta operación es computacionalmente costoso, especialmente cuando las funciones a correlacionar son extensas, y además implica la necesidad de un muestreo, con los inconvenientes que esto acarrea. Por otro lado, los sistemas ópticos pueden realizar correlaciones a la velocidad de la luz, sin importar el tamaño de las funciones a correlacionar y sin necesidad de discretizarlas. Los correladores son usados en detección de diagramas y seguimiento de objetivos en imágenes. El primer correlador propuesto fue el denominado filtro de Vander Lugt en honor a su inventor [19], seguido dos años después por el JTC, demostrado por Weaver & Goodman [20].

La gran contribución de Refrieger & Javidi fue demostrar que la aplicación de los correladores ópticos a funciones de fase aleatorias da lugar a la posibilidad de encriptar la información. Por otro lado, es posible ver que tanto los correladores ópticos como los sistemas DRPE tienen una estrecha relación con la holografía. Recordemos la forma de un holograma de Fourier fuera de eje

$$H(v,w) = |O(v,w)|^2 + |R(v,w)|^2 + O(v,w)R^*(v,w) + O^*(v,w)R(v,w) \tag{2.2.1}$$

Donde $O(v,w)$ era la transformada de Fourier de la luz dispersada por un objeto $o(x,y)$ y $R(v,w)$ es una onda de referencia de la forma

$$R(v,w) = re^{-2\pi i\lambda f(v\sin\phi)} \tag{2.2.2}$$

con f la distancia focal de la lente que realiza la TF, y las coordenadas v, w dadas por [21]

$$v = \frac{x}{\lambda f}; \qquad w = \frac{y}{\lambda f} \tag{2.2.3}$$

Ahora bien, supongamos que la luz proveniente del objeto interfiere con la transformada de Fourier $F(v,w)$ de otro objeto o función $f(x,y)$ en lugar de con la onda plana $R(v,w)$, manteniendo el mismo ángulo entre las ondas. Al realizar la TFI de (2.2.1) con esta suposición obtenemos

$$\begin{aligned} h(x,y) = {} & o(x,y) \otimes o^*(x,y) + f(x,y) \otimes f^*(x,y) \\ & o(x,y) \otimes f^*(x,y) \otimes \delta\left(x - \frac{\sin\phi}{\lambda}\right) + \\ & o^*(x,y) \otimes f(x,y) \otimes \delta\left(x + \frac{\sin\phi}{\lambda}\right) \end{aligned} \tag{2.2.4}$$

la ecuación (2.2.4) muestra que la reconstrucción de un holograma de Fourier al cambiar la onda de referencia por una función arbitraria, consiste en un orden central, donde aparecen las autocorrelaciones de $o(x,y)$ y $f(x,y)$, y las correlaciones entre estas dos funciones, con una separación espacial dada por el ángulo ϕ. De esta manera, los sistemas holográficos fuera de eje pueden considerarse correladores ópticos.

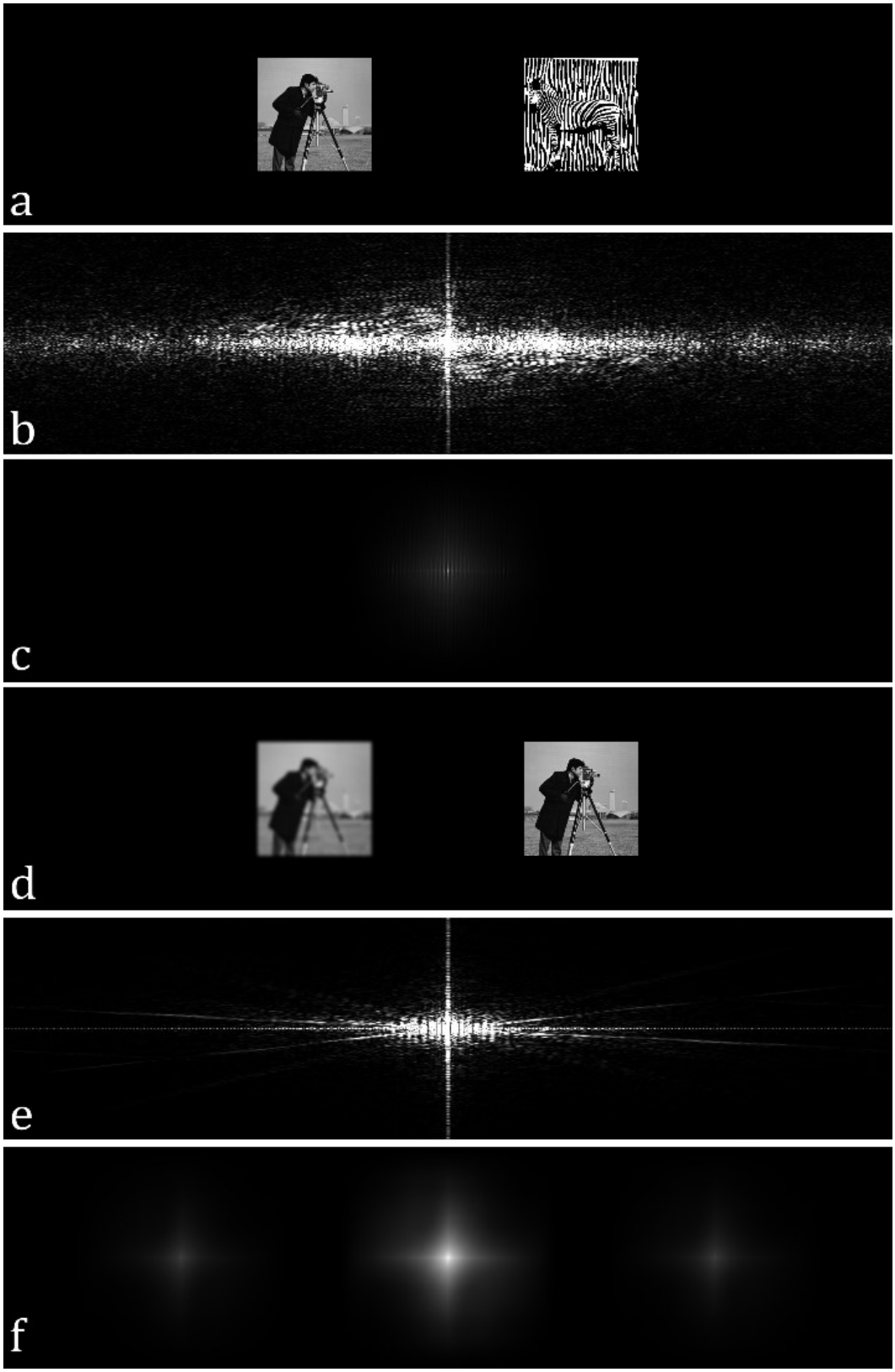

Figura 22: Correlación holográfica entre dos imágenes. a) imágenes a correlacionar, b) holograma, c) reconstrucción óptica de b), d) imágenes a correlacionar, e) holograma, y f) reconstrucción óptica de e).

En la Figura 22 se muestra el resultado de realizar correlaciones con un sistema holográfico de Fourier como el descrito anteriormente. En este caso, cuando las funciones $o(x,y)$ y $f(x,y)$ a correlacionar son diferentes (Figura 22.a), tras reconstruir el holograma correspondiente (Figura 22.b) sólo se observa el orden central, ya que la correlación entre las dos funciones es baja (Figura 22.c). Por el contrario, si ambas funciones son similares como en la Figura 22.d, aparecen picos intensos correspondientes a la correlación de las funciones (Figura 22.e) en una posición que dependerá del ángulo de incidencia entre las ondas a la hora de registrar el holograma, como se describe en la ecuación (2.2.4). Esta propiedad hace a los correladores útiles para comparar imágenes o para el seguimiento de datos en una escena.

Si deseamos reconstruir un objeto, basta imponer la condición de que $f(x,y)$ sea tal que

$$o(x,y) \otimes f^{*}(x,y) \approx o(x,y) \tag{2.2.5}$$

de la condición anterior podemos deducir que la reconstrucción será perfecta cuando $f(x,y)$ sea una delta de Dirac, como ocurre con la TF de una la onda plana ideal. Desde este punto de vista, $f(x,y)$ es la función respuesta al impulso del sistema holográfico, y al igual que en los sistemas de formación de imágenes, si la función $f(x,y)$ difiere de una delta de Dirac, producirá una reconstrucción menos fiel al objeto $o(x,y)$.

Conociendo la condición (2.2.5), nos podemos preguntar qué otra función $F(v,w)$ cumple la condición de que su TFI sea igual a una delta de Dirac. En el caso de la encriptación, la respuesta a esta pregunta es la intensidad de una función compleja aleatoria $K(v,w)$, tal que

$$\begin{aligned} f(x,y) &= TFI[|K(v,w)|^2] \\ f(x,y) &= k(x,y) \otimes k^{*}(x,y) \end{aligned} \tag{2.2.6}$$

cómo $K(v,w)$ es una función aleatoria, $k(x,y)$ también lo es, y su autocorrelación puede ser tomada aproximadamente igual a una delta de Dirac, siempre y cuando $k(x,y)$ tenga una extensión infinita en el espacio. A esta aproximación se le denomina aproximación de ruido blanco de gran ancho de banda [22]. Ahora bien, ¿qué ocurre si realizamos la correlación entre el objeto que deseamos reconstruir y la función aleatoria

$K(v,w)$ en lugar de su intensidad? Según la ecuación (2.2.4) obtendremos la correlación del objeto con $k(x,y)$ y su complejo conjugado. La correlación entre el objeto y una función aleatoria como lo es $k(x,y)$ produce una reconstrucción casi irreconocible, ocultando la información del objeto $o(x,y)$. El holograma de Fourier que resulta en esta correlación esta dado por

$$H(v,w) = |O(v,w)|^2 + |R(v,w)|^2 + O(v,w)K^*(v,w) + O^*(v,w)K(v,w) \tag{2.2.7}$$

Ahora bien, si multiplicamos este holograma por $K(v,w)$, tras realizar la ITF del producto resultante, obtendremos de nuevo el objeto reconstruido correctamente, siempre y cuando se cumpla la aproximación de gran ancho de banda para $k(x,y)$. De esta manera, hemos convertido un correlador óptico, como lo es un sistema de holografía de Fourier, en un sistema de encriptación, donde la función $K(v,w)$ es la llave de seguridad sin la cual no es posible reconstruir el objeto.

El argumento anterior muestra porque los sistemas DRPE se basan en correladores, ya sea el 4f o el JTC, sin embargo, Refregier & Javidi fueron más restrictivos en su trabajo seminal. Ellos plantearon que el DRPE usara dos máscaras de solo fase, una como llave y otra multiplicando el objeto. El propósito de usar dos máscaras es garantizar que la reconstrucción del objeto sea indistinguible de un diagrama de ruido blanco, independientemente de la estructura del objeto a ser encriptado, garantizando así la seguridad de la encriptación. Usar solo una máscara aleatoria hace el objeto irreconocible, pero dependiendo de la estructura de éste es posible identificar alguna de sus características.

En la Figura 23 se compara la correlación de una imagen (Figura 23.a) con una función de fase aleatoria (Figura 23.c) con la misma correlación, pero multiplicando la imagen de entrada con otra función de fase aleatoria (Figura 23.f). Como mencionamos previamente, la correlación con una sola mascara no permite reconocer claramente la imagen, pero algunas características pueden deducirse, por ejemplo, la presencia de franjas en la misma. En cambio, al multiplicar el objeto de entrada por otra función de fase aleatoria, el resultado de la correlación es un ruido blanco sin ninguna estructura identificable. Usar funciones de fase en vez de funciones complejas permite que la intensidad del objeto no se vea afectada por la multiplicación con la función aleatoria.

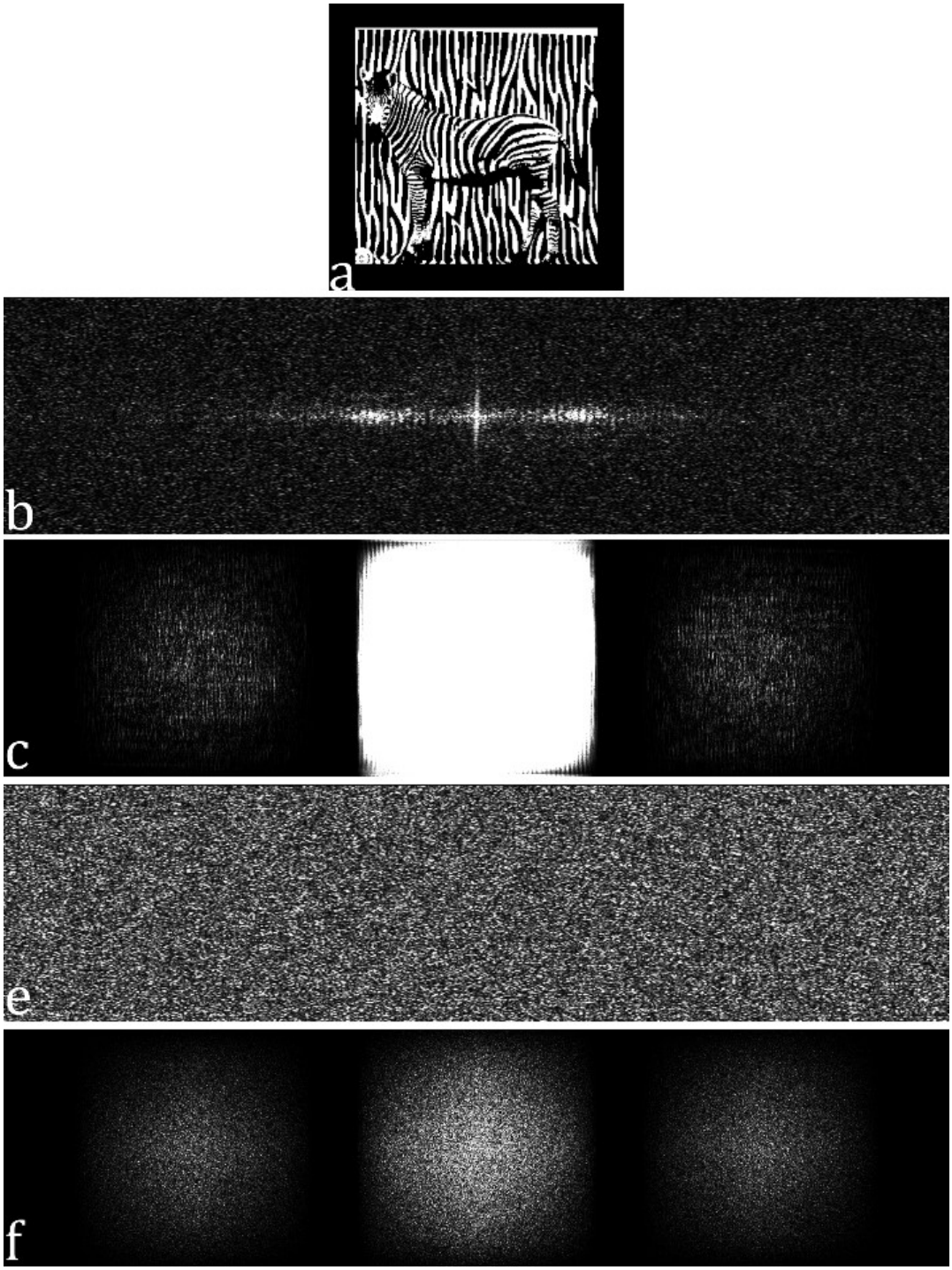

Figura 23: Correlación con funciones de fase aleatorias. a) objeto de entrada, b) holograma con una función de fase aleatoria, c) reconstrucción del holograma b), e) holograma con doble función de fase aleatoria, y f) reconstrucción del holograma e).

2.3. Criptosistema de correlador de transformada conjunta

La encriptación usando el sistema JTC se logra de la misma forma que la deducida en la sección anterior para un correlador basado en un sistema de holografía de Fourier fuera de eje. La principal diferencia radica en que las dos funciones a ser correlacionadas se ubican en el mismo plano, separadas por una distancia $2b$, y que en el plano de la cámara se registra la interferencia entre las transformada de Fourier de ambas funciones, no solo del objeto. En esta configuración, se minimiza la diferencia de camino óptico entre la luz proveniente de ambas funciones u objetos, lo que garantiza la posibilidad de un registro holográfico efectivo sin necesidad de fuentes de alta longitud de coherencia.

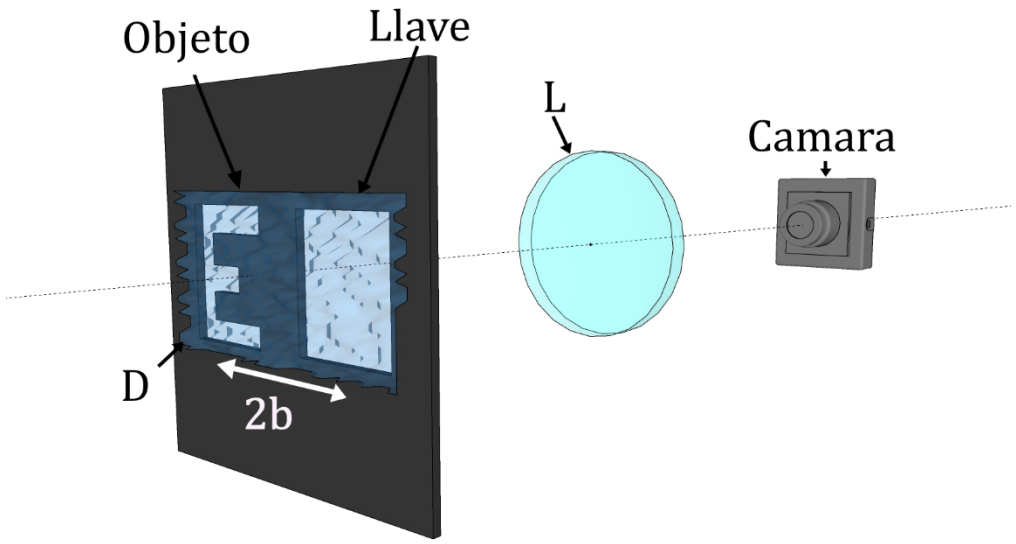

Figura 24: Esquema de un criptosistema JTC. L: lente, D: difusor.

Para la encriptación, una función es el objeto por encriptar, y la otra es la máscara aleatoria que sirve de llave. En la implementación experimental de este sistema, el plano de entrada se genera con un elemento de amplitud como una diapositiva o modulador de amplitud en el cual se ubica el objeto a encriptar y una pupila o ventana. En contacto con este elemento de amplitud se pone un difusor, el cual provee las funciones de fase aleatorias que multiplican al objeto y de la llave.

La cámara registra el "holograma" resultante de la interferencia entre la transformada de Fourier del objeto y la llave, el cual se denomina en este sistema espectro conjunto de

potencias (JPS por las siglas de su nombre en inglés "joint power spectrum"). Este está dado por

$$U(v,w) = \left|C(v,w)\right|^2 + \left|K(x,y)\right|^2 + C^*(v,w)K(v,w)e^{4\pi ibv} + C(v,w)K^*(v,w)e^{-4\pi ibv} \tag{2.3.1}$$

Donde $C(v,w)$, $K(v,w)$ son las TFs de $c(x,y) = o(x,y)r(x,y)$ y $k(x,y)$, siendo $o(x,y)$ el objeto a encriptar, y $r(x,y)$, $k(x,y)$ máscaras aleatorias de fase. Al igual que en los hologramas de Fourier, en el plano de reconstrucción los términos de la ecuación (2.3.1) tendrán una separación dependiente de la distancia $2b$ entre el objeto y la llave. Este JPS contiene el dato encriptado, junto con información no deseada que reduce la calidad de la desencriptación y hace más vulnerable el sistema. Esta información extra puede eliminarse aplicando el proceso de filtrado descrito en la sección 1.5, lo cual equivale a eliminar los primeros 3 términos de la ecuación (2.3.1), dejando sólo el correspondiente al objeto encriptado.

$$E(v,w) = C(v,w)K^*(v,w) \tag{2.3.2}$$

Tal y como se explicó en la sección anterior, es necesario multiplicar el objeto encriptado por $K(v,w)$ para lograr la reconstrucción. Tras hacer la TFI de este producto se obtiene

$$d(x,y) = c(x,y) \otimes k^*(x,y) \otimes k(x,y) \tag{2.3.3}$$

Si se aplica la aproximación $k^*(x,y) \otimes k(x,y) \approx \delta(x,y)$, vemos que la ecuación anterior corresponde al objeto reconstruido correctamente.

Debido a que la desencriptación requiere la TF de la llave $K(v,w)$, en la implementación experimental se debe registrar la misma. Como $K(v,w)$ es una función compleja, su registro implica utilizar una técnica holográfica. A continuación mostraremos un sistema de encriptación JTC con holografía digital de Fourier, tal y como fue reportado por Rueda et al [23]. En este esquema, el plano de entrada JTC es proyectado en un modulador espacial de luz (SLM por sus siglas en inglés "spatial light modulator"). Este tipo de sistema puede ser usado para encriptar objetos 2D, como mensajes cortos o imágenes.

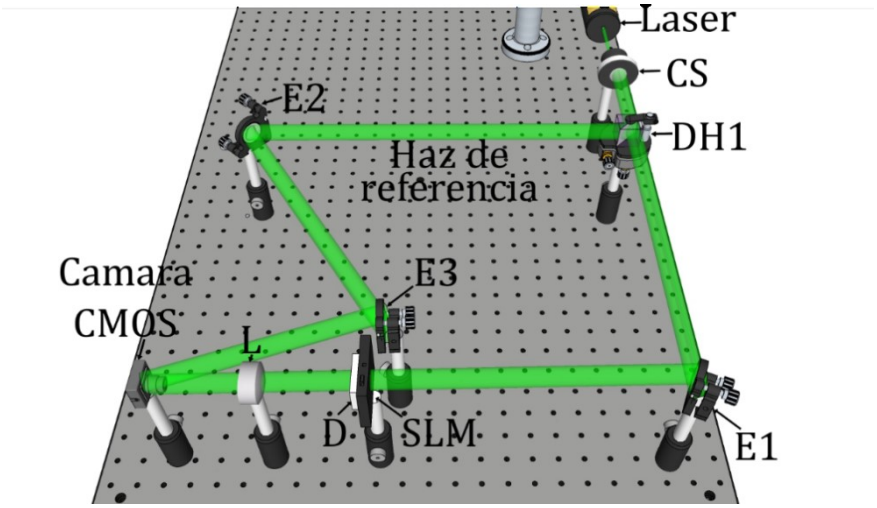

Figura 25: Esquema experimental de un sistema de encriptación JTC. CS: sistema de colimación, DH: divisor de haz, E: espejo, L: lente, D: difusor, SLM: modulador espacial de luz.

El esquema del sistema experimental opto digital JTC se muestra en la Figura 25. En este sistema el registro del JPS se logra simplemente bloqueando el haz de referencia y proyectando el plano de entrada del JTC en el modulador espacial de luz. La llave $k(x,y)$ se registra por medio de un holograma digital de Fourier. Para esto, se proyecta en el modulador únicamente la ventana de la llave y se desbloquea el haz de referencia. El holograma resultante se filtra usando la técnica descrita en la sección 1.5.

Para la realización de este sistema se usó como fuente de iluminación un láser de Nd:YAG Coherent con longitud de onda de 532 nm y 300 mW de potencia. El medio de registro fue una cámara CMOS EO-10012C con resolución de 3840x2748 y tamaño de pixel de $1.67\ \mu m \times 1.67\ \mu m$. El plano de entrada del sistema JTC fue proyectado en un modulador modelo Holoeye LC-2002, el cual tiene 800x600 pixeles de resolución y un tamaño de pixel de $32\ \mu m \times 32\ \mu m$. El objeto por encriptar y la llave tienen dimensiones de $12.8\ mm \times 12.8\ mm$. La lente usada para realizar la TF es de $200\ mm$ de longitud focal.

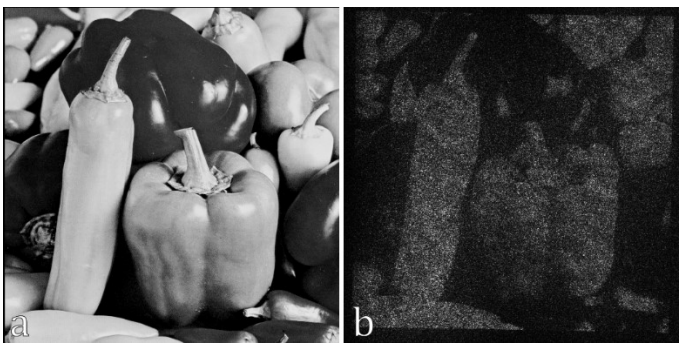

Figura 26: Proceso de encriptación-desencriptación experimental. a) objeto de entrada, b) objeto desencriptado.

En la Figura 26 se muestra un resultado típico obtenido con un sistema JTC experimental. Como se puede apreciar, el objeto desencriptado presenta una considerable degradación respecto al objeto original. En secciones posteriores estudiaremos el motivo de esta degradación y propondremos algunas respuestas para mitigarla.

2.4. Encriptación en el dominio de Fresnel.

Una de las características deseables en los sistemas de encriptación es la existencia de múltiples parámetros de seguridad. Un parámetro de seguridad es una información sobre el método de encriptación, adicional a la llave, que un usuario debe conocer para poder llevar a cabo una desencriptación exitosa. La búsqueda de nuevos parámetros de seguridad, aplicada a los sistemas ópticos de encriptación, llevó a explorar sistemas basados en transformaciones alternativas, en lugar de la transformada de Fourier. La implementación más simple de esta idea es el sistema de encriptación en el dominio de Fresnel. En este sistema, la correlación entre dos funciones aleatoria para lograr la encriptación se obtiene por medio de la transformada de Fresnel, es decir, por la propagación de la luz en el espacio libre.

El primer sistema de este tipo fue implementado por G. Situ & J. Zhang en el 2004 [24]. El sistema planteado por Situ es similar a la implementación original del DRPE basado en el sistema 4F. En este esquema, en el plano de entrada se ubica el objeto en contacto con una primera máscara de fase aleatoria. La luz proveniente del plano de entrada se propaga libremente una distancia d_1 hasta llegar a una segunda mascara de fase, tras lo cual continúa propagándose otra distancia d_2.

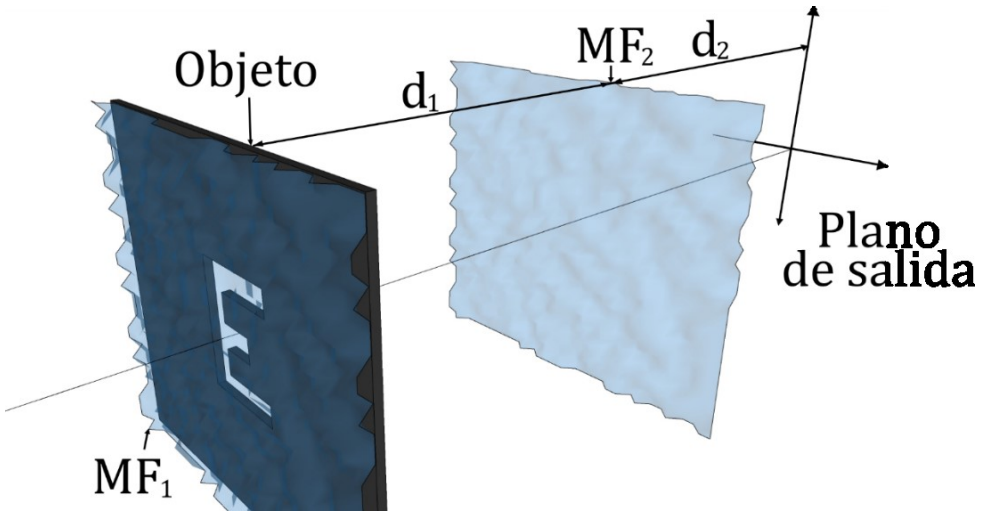

Figura 27: Esquema del sistema DRPE en el dominio de Fresnel propuesto por Situ & Zhang. MF: mascara de fase aleatoria.

En la Figura 27 se muestra el esquema del sistema DRPE en el dominio de Fresnel descrito anteriormente. Para desencriptar, el usuario debía realizar la transformada de Fresnel inversa una distancia d_2, multiplicar por la máscara de fase 2, y luego realizar otra transformada de Fresnel inversa una distancia d_1. Este sistema, al igual que el criptosistema 4f que lo inspiró, presenta el inconveniente de que el objeto encriptado es una función compleja, lo que implica que su registro debe efectuarse por medio de un sistema holográfico, como fue propuesto originalmente. Adicionalmente, el sistema requiere gran precisión para garantizar la alineación óptima entre las máscaras a la hora de desencriptar.

Estas limitaciones hicieron deseable el uso de un sistema de transformada conjunta en el dominio de Fresnel, el cual tuviera características semejantes a las del sistema JTC, pero conservando la posibilidad de usar la distancia de propagación de la luz como un parámetro de seguridad.

La Mela e Iemmi [25] mostraron un sistema de encriptación en el dominio de Fresnel que hace uso de la arquitectura JTC, en el cual se usa holografía en línea con phase shifting para registrar la información de la llave de encriptación. Trabajos posteriores presentaron modificaciones a este sistema, en el cual se usa holografía fuera de eje para el registro de la información de la llave y se implementan modificaciones no lineales para mejorar su seguridad [26].

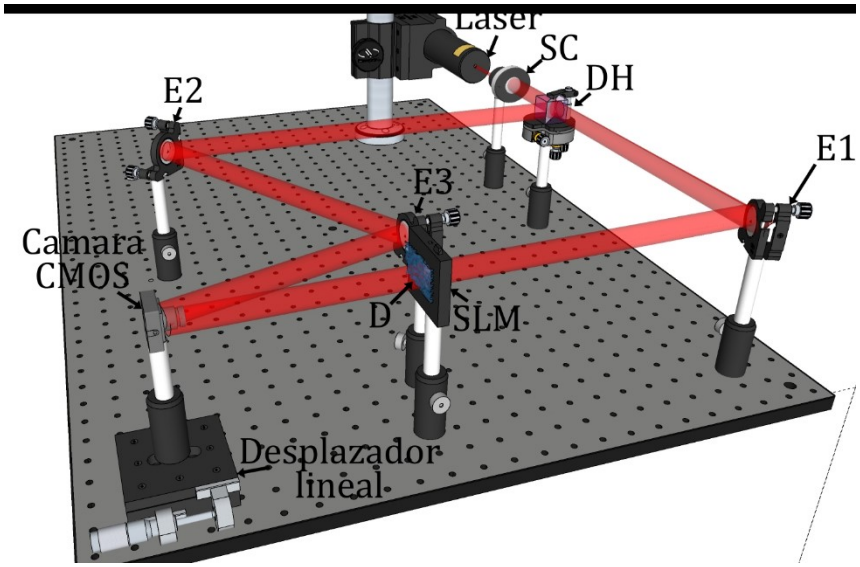

Figura 28: Criptosistema basado en la propagación libre conjunta. E: espejo, DH: divisor de haz, SC: sistema de colimación, SLM: modulador espacial de luz, D: difusor.

Jaramillo et al [24] implementaron un sistema de este tipo, el cual fue denominado criptosistema de propagación libre conjunta (JFSC por las siglas en ingles de joint free space cryptosystem), el cual se muestra en la Figura 28. En el JFSC el plano de entrada está conformado, al igual que en el JTC, por una ventana o pupila que junto con el difusor sirve de llave, y el objeto, separados una distancia $2b$ (ver Figura 24). Para encriptar, se bloquea el brazo de referencia, y el medio de registro. En este caso una cámara CMOS, captura la denominada distribución de potencias conjuntas de Fresnel (JFPD por las siglas en inglés de joint Fresnel power distribution), la cual es la intensidad de la luz que se propaga desde el plano de entrada hasta la cámara. De la misma manera que el JPS en un sistema JTC puede considerarse un holograma de Fourier donde la onda de referencia es la TF de una máscara aleatoria de fase, el JFPD es un holograma de Fresnel donde la onda de referencia es la transformada de Fresnel de una máscara aleatoria de fase.

Sea z la distancia entre el plano de entrada y el medio de registro, entonces el JFPD está descrito por

$$I(v,w) = |C_z(v,w)|^2 + |L_z(v,w)|^2 + C_z(v,w)L_z^*(v,w)e^{-4\pi ibv} + C_z^*(v,w)L_z(v,w)e^{4\pi ibv} \quad (2.4.1)$$

Donde $C_z(v,w)$ y $L_z(v,w)$ son las transformadas de Fresnel correspondientes a la propagación de la luz proveniente de la ventana de la llave y del objeto hasta la cámara

CMOS. Las coordenadas en el espacio de Fresnel están dadas por $v = x/\lambda z$ y $w = y/\lambda z$, con λ la longitud de onda.

Como se mencionó anteriormente, el JFPD es en esencia un holograma de Fresnel, y presenta franjas de interferencia cuya frecuencia dependen de la separación entre la ventana llave y el objeto en el plano de entrada. El tamaño de pixel Δx del medio de registro impone un límite a esta distancia, el cual es dado por

$$b = \tan\left(\sin^{-1}\left(\frac{\lambda}{4\Delta x}\right)\right) \tag{2.4.2}$$

Ahora procedemos a eliminar los términos responsables del orden central y la imagen gemela del JFPD. Este proceso es análogo al filtrado de un holograma de Fresnel descrito en la sección 1.5. Tras realizar el filtrado obtenemos el objeto encriptado, dado por

$$E_z(v,w) = C_z(v,w)L_z^*(v,w) \tag{2.4.3}$$

Al igual que en el sistema JTC, para desencriptar simplemente se multiplica el objeto encriptado por $L_z(v,w)$ y se aplica una TFrI, tras lo cual se obtiene

$$d(x,y) = c(x,y) \otimes l^*(x,y) \otimes l(x,y) \tag{2.4.4}$$

Como $l(x,y)$ es una máscara de fase aleatoria, se puede aplicar la aproximación de ruido blanco de gran ancho de banda, haciendo $l^*(x,y) \otimes l(x,y) \approx \delta(x,y)$, obteniendo así el objeto desencriptado $c(x,y)$.

Para poder desencriptar, es necesario tener la función $L_z(v,w)$. Para registrar digitalmente esta función se procede de forma análoga al sistema JTC con holografía digital expuesto en la sección anterior. Se proyecta en el SLM únicamente la ventana de la llave y se desbloquea el brazo de referencia. La cámara CMOS registra el holograma de Fresnel de $l(x,y)$, a partir del cual se puede obtener $L_z(v,w)$ tras un proceso de filtrado.

A continuación, probamos experimentalmente el desempeño del JFSC. Para ello, se implementó el sistema de la Figura 28. Todos los datos experimentales de esta sección fueron registrados usando una cámara CMOS EO-10012M con un tamaño de pixel de 1.67 $\mu m \times 1.67\ \mu m$ y una resolución de 3840×2748 pixeles. La fuente de iluminación fue un láser de estado sólido bombeado por diodo con una longitud de onda de 532 nm y 300

mW de potencia. La ventana de la llave y el objeto tienen tamaño máximo de 3.2 mm × 3.2 mm con una separación entre ambos de 3.87 mm. El plano de entrada fue proyectado en un SLM Holoeye 2002 con una resolución de 800×600 pixeles y tamaño de pixel de $32\ \mu m \times 32\ \mu m$. Para las pruebas de desplazamiento axial se usó un desplazador lineal de 50 cm de longitud.

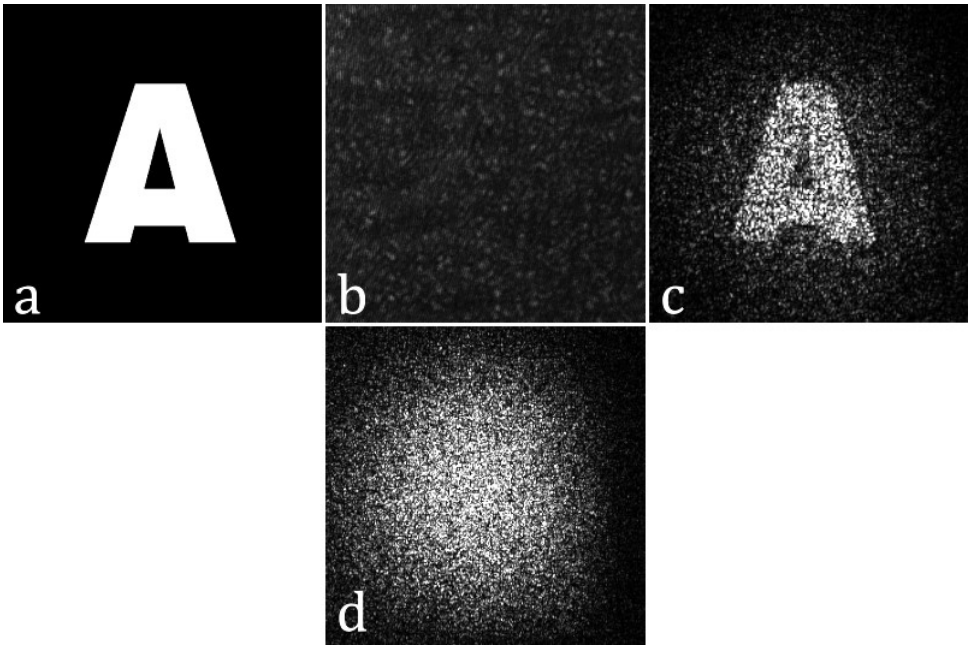

Figura 29: Resultados experimentales de encriptación-desencriptación con un JFSC. a) objeto de entrada, b) JFPD, c) objeto desencriptado con la llave y transformada de Fresnel correctas, y d) objeto desencriptado con la llave incorrecta y transformada de Fresnel correcta.

En la Figura 29 mostramos resultados experimentales obtenidos con el JFSC. Al igual que un sistema DRPE convencional, cuando se usa una llave incorrecta, aun si se desencripta con la transformada de Fresnel correcta, el resultado es ruido blanco aleatorio, como se muestra en la figura Figura 29d. Para estos resultados la distancia entre el plano de entrada y de salida fue z=350 mm.

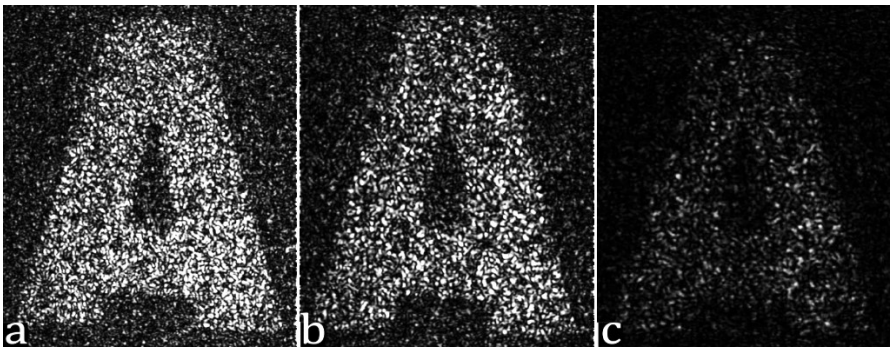

Figura 30: Desencriptación correcta de objetos encriptados con el JFSC usando distancias objeto cámara de a) 250 mm b) 300 mm y c) 350 mm.

En la Figura 30 mostramos resultados del proceso de encriptación-desencriptación obtenidos con el JFSC manteniendo la ganancia de la cámara CMOS constante. Como se puede apreciar, al aumentar la distancia entre el objeto y la cámara, hay una disminución en la intensidad del objeto reconstruido y un aumento en su tamaño de speckle. Esto se debe a que el área limitada de la cámara registra menos luz, comportándose como una pupila. Este efecto se traduce en una reducción de la calidad del objeto desencriptado.

Para verificar esta degradación, calculamos el error cuadrático medio normalizado (NMSE por las siglas en ingles de "normalized mean square error") entre los objetos desencriptados a partir de JFPDs obtenidos con diferentes distancias cámara-objeto $m_z(p,q)$ y el objeto original $m(p,q)$. El NMSE es definido como

$$NMSE = \frac{\sum_{p,q}^{N,M} |m(p,q) - m_z(p,q)|^2}{\sum_{p,q}^{N,M} |m(p,q) - m_w(p,q)|^2} \qquad (2.4.5)$$

Donde (p,q) son las coordenadas de pixel, N y M son el número de pixeles horizontales y verticales de la imagen recuperada y $m_w(p,q)$ es el peor caso obtenido.

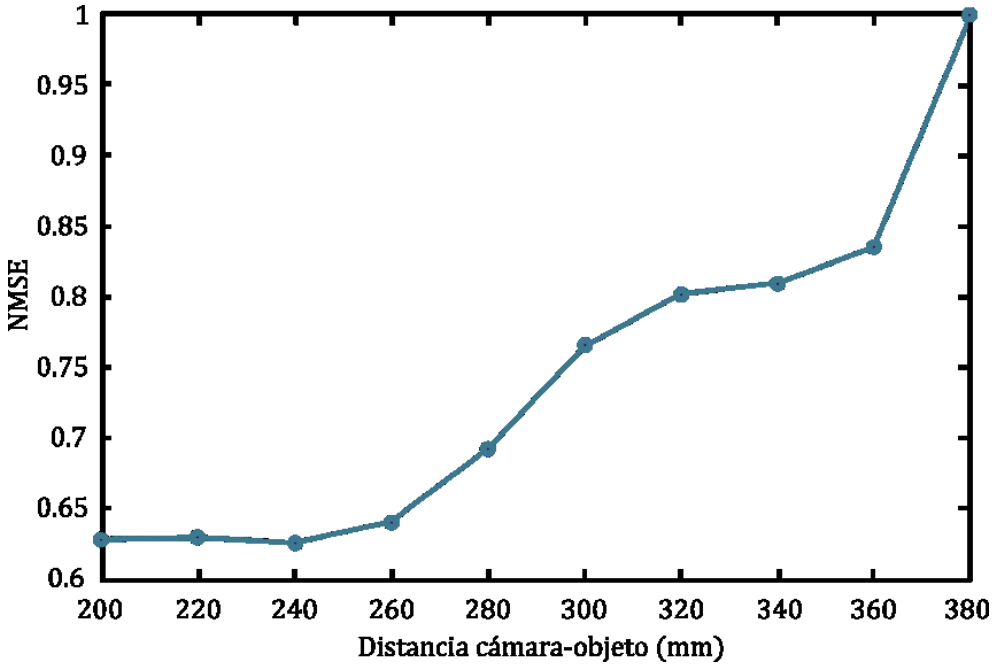

Figura 31: NMSE de los objetos desencriptados usando JFPD registrados a diferentes distancias cámara objeto.

Los resultados de la Figura 31 demuestran el efecto de aumentar la distancia cámara objeto. Al igual que en los resultados de la Figura 30, el aumento en la distancia se traduce

en un aumento en el error del objeto desencriptado. En este sentido, el JFSC tiene un rango de operación limitado.

Finalmente, procedimos a probar el desempeño de la distancia cámara objeto como parámetro de seguridad. Un parámetro de seguridad ideal es aquel que permite desencriptación si y solo si se usa el valor exacto del mismo, aun si se tiene la llave correcta. En el caso del JFSC, la distancia es un parámetro de seguridad si solo permite desencriptar cuando se usa la transformada de Fresnel inversa correspondiente a la distancia exacta a la que se registró el JFPD, tras multiplicar el objeto encriptado por la llave.

Para probar esto, se intentó desencriptar un dato encriptado usando la llave correcta, pero realizando una TFrI con diferentes distancias. El objeto fue encriptado con una distancia de $z = 350mm$. Se calculo el NMSE entre el objeto original y el desencriptado con los distintos valores de z.

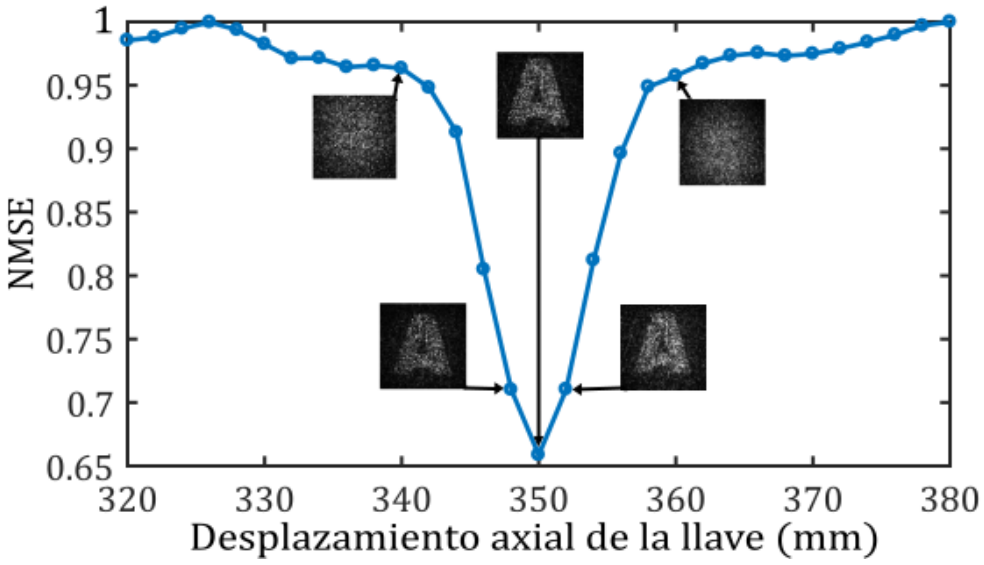

Figura 32:NMSE del objeto desencriptado usando diferentes valores de la distancia cámara-objeto.

El resultado de esta prueba se muestra en la Figura 32. Como se puede apreciar por las imágenes insertadas en la gráfica, existe una tolerancia de aproximadamente un centímetro a la hora de desencriptar con valores distintos de la distancia de propagación a la que fue encriptado el objeto. Esta tolerancia indica que la distancia no es un parámetro de seguridad ideal, por lo que los sistemas de encriptación en el dominio de Fresnel ofrecen mayor flexibilidad en la implementación experimental, pero no necesariamente son más seguros que los sistemas DRPE convencionales, ya que un

atacante si adquiere la llave de seguridad, puede lograr desencriptación correcta aun si carece de la distancia objeto-llave adecuada, simplemente realizando propagaciones sucesivas.

2.5. Encriptación en el dominio Fraccional.

El sistema DRPE fue concebido como una aplicación de los correladores, como mencionamos anteriormente, sin embargo, conforme empezaron a investigarse distintas arquitecturas de encriptación óptica, cobro interés el planteamiento de un marco teórico unificado para el estudio de los sistemas DRPE. Una de las formas de lograr esta unificación se dio a través de la denominada transformada fraccional de Fourier (TFrF) [27]. La TFrF es una generalización matemática de la transformada de Fourier, la cual tiene como característica el llamado orden fraccional. Si la transformada de Fourier conecta variables conjugadas como el espacio y la frecuencia, la transformada fraccionaria permite una rotación continua entre las dos representaciones. La transformada fraccionaria de Fourier está definida como

$$F_{\alpha}\left[f(x)\right]=\frac{e^{i\left(\frac{\pi}{4}-\frac{\alpha}{2}\right)}}{\sqrt{2\pi\sin(\alpha)}}e^{\left(-\frac{i}{2}\cot\alpha v^{2}\right)}\int_{-\infty}^{\infty}e^{\left(-\frac{i}{2}\cot\alpha x^{2}+\frac{ixv}{\sin\alpha}\right)}f(x)dx \tag{2.5.1}$$

y la transformada fraccionaria de Fourier inversa (TFrFI) es dada por

$$F_{-\alpha}\left[f(x)\right]=\frac{e^{i\left(\frac{\pi}{4}-\frac{\alpha}{2}\right)}}{\sqrt{2\pi\sin(\alpha)}}e^{\left(\frac{i}{2}\cot\alpha v^{2}\right)}\int_{-\infty}^{\infty}e^{\left(\frac{i}{2}\cot\alpha x^{2}-\frac{ixv}{\sin\alpha}\right)}f(x)dx \tag{2.5.2}$$

donde α es el llamado orden fraccionario, y toma un valor entre $-\pi/2$ y $\pi/2$. Las definiciones anteriores se reducen a la transformada de Fourier común y su inversa cuando el orden fraccionario es $\pi/2$ y $-\pi/2$ respectivamente. El efecto de la transformada de Fourier fraccional sobre una imagen se muestra en la Figura 33.

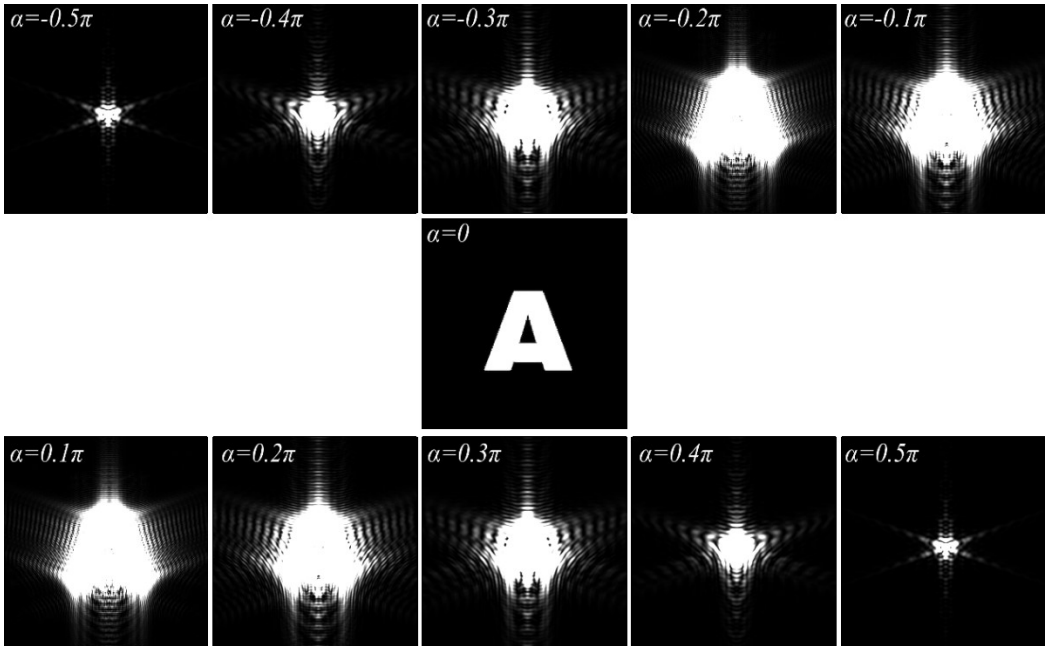

Figura 33: Transformada fraccional de Fourier de una letra A para distintos órdenes fraccionales.

La TFrF mantiene las propiedades de desplazamiento y convolución de la transformada de Fourier convencional [28], y además se puede implementar ópticamente, a diferencia de muchas otras transformaciones lineales canónicas [29,30]. Existen diversas formas de lograr TFrF ópticamente, pero en este caso nos centraremos en un sistema de una lente con distancias plano entrada-lente y lente-plano de salida variables.

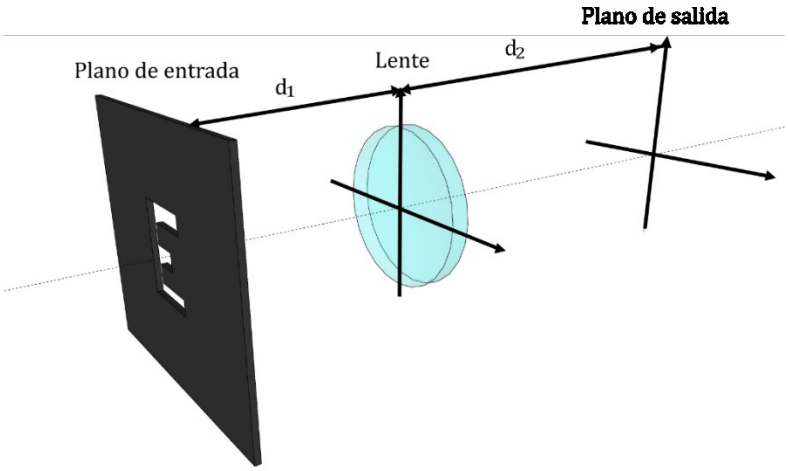

Figura 34: Esquema utilizado para la transformada fraccionaria de Fourier óptica.

En la Figura 34 se muestra el esquema que aplicamos para la implementación óptica de la TFrF. El orden de la TFrF que se realiza con el mismo se relaciona con los parámetros ópticos del sistema con la siguiente ecuación [31]

$$\alpha = \cos^{-1}\left(\frac{\sqrt{(d_1 - f)(d_2 - f)}}{f}\right) \qquad (2.5.3)$$

Donde d_1 es la distancia plano de entrada-lente, d_2 es la distancia lente-plano de salida y f es la distancia focal del lente. Teniendo en cuenta el esquema descrito para realizar la TFrF, un correlador óptico fraccionario puede implementarse simplemente tomando el JTC convencional y variando las distancias entre la lente, el plano de entrada y el plano de salida [32] como lo indica la ecuación (2.5.3). De la misma manera, también es posible registrar hologramas fraccionales usando un esquema de holografía de Fourier con cambio en estos parámetros.

Teniendo en cuenta estas posibilidades, la implementación de un sistema DRPE fraccional fue propuesto por primera vez en el año 2000 por Unnikrishnan *et al* [33]. Este sistema era en esencia una variación del sistema 4f modificado para realizar la encriptación por medio de la correlación de dos máscaras de fase aleatorias usando la TFrF. Al estar basado en el sistema 4f, este sistema conserva las mismas exigencias de alineación y la necesidad de un registro holográfico del objeto encriptado.

Estas limitaciones dieron lugar a la posterior implementación del DRPE con arquitectura JTC [34]. Al igual que el JFSC, el criptosistema JTC fraccional (FrJTCC por las siglas en ingles de “Fractional Joint Transform Correlator cryptosystem”), presenta un parámetro nuevo que puede contribuir a la seguridad del sistema, el orden fraccional. Para determinar el desempeño de este parámetro de seguridad, implementamos un FrJTCC con holografía digital fraccionaria [35], como se muestra en el esquema de la Figura 35.

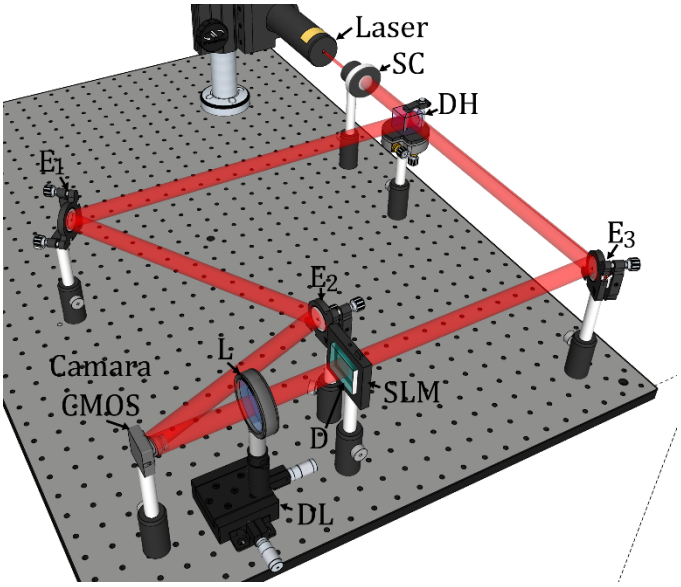

Figura 35: Esquema de un FrJTCC con holografía digital fraccionaria. E: espejo, SC: sistema de colimación, D: difusor, DH: divisor de haz, L: lente, DL: desplazador lineal, SLM: modulador espacial de luz.

En este sistema, el plano de entrada tiene la misma forma que en el criptosistema JTC convencional, con una ventana llave y otra donde se proyecta el objeto, separadas una distancia $2b$. Este plano de entrada es proyectado en un SLM, el cual está en contacto con un difusor que proveerá las máscaras aleatorias de fase. Una lente de distancia focal f está ubicada a una distancia d_1 del modulador, y a una distancia d_2 de la cámara CMOS. En el plano de salida se obtiene una TFrF del plano de entrada cuyo orden fraccional esta dado por la ecuación (2.5.3). A la intensidad de esta transformación, que es registrada por la cámara CMOS, se le denomina distribución de potencias conjuntas fraccionarias (JFrPD por las siglas en ingles de "joint fractional power distribution"). El JFrPD es dado por

$$\begin{aligned} I_\alpha(v,w) = &| c_\alpha(v,w)|^2 + | l_\alpha(v,w)|^2 + c_\alpha(v,w) l^*{}_\alpha(v,w)\, \mathrm{e}^{-4\pi b v \csc(\alpha)} \\ &+ c^*{}_\alpha(v,w) l_\alpha(v,w)\, \mathrm{e}^{4\pi b v \csc(\alpha)} \end{aligned} \qquad (2.5.4)$$

Donde $c_\alpha(v,w)$ y $l_\alpha(v,w)$ son las TFrF con orden α del objeto $c(x,y)$ y la llave $l(x,y)$. El JFrPD contiene el objeto encriptado, además de términos adicionales que pueden afectar la calidad de la desencriptación e incrementar la vulnerabilidad del sistema. Para evitar esto, aplicamos el mismo proceso de filtrado digital que se aplicó a los hologramas de Fourier, Fresnel y los JPS y JFPD obtenidos con los sistemas de encriptación usados en las secciones anteriores. Seleccionando el tercer término de la ecuación (2.5.4) y descartando los remanentes, obtenemos el objeto encriptado dado por

$$E_\alpha(v,w) = c_\alpha(v,w) l_\alpha(v,w) \tag{2.5.5}$$

Para lograr la desencriptación se procede de forma análoga al JFPD, primero se multiplica el objeto encriptado por $l_\alpha(v,w)$ y luego se realiza una transformada fraccionaria de Fourier inversa, correspondiente al orden fraccional α. La información de $l_\alpha(v,w)$ se registra digitalmente proyectando solo la ventana de la llave y desbloqueando el haz de referencia, dado por

$$P(v,w) = e^{-2\pi i\lambda(v\sin(\theta)+w\sin(\phi))} \tag{2.5.6}$$

obteniendo así un holograma fraccional de la ventana de la llave, descrito como

$$\begin{aligned} H_\alpha(v,w) = & |l_\alpha(v,w)|^2 + 1 \\ & + l_\alpha(v,w) e^{-2\pi i\lambda(v\sin(\theta)+w\sin(\phi))} + l_\alpha(v,w) e^{2\pi i\lambda(v\sin(\theta)+w\sin(\phi))} \end{aligned} \tag{2.5.7}$$

De este holograma se puede extraer la información de $l_\alpha(v,w)$ tras un proceso de filtrado.

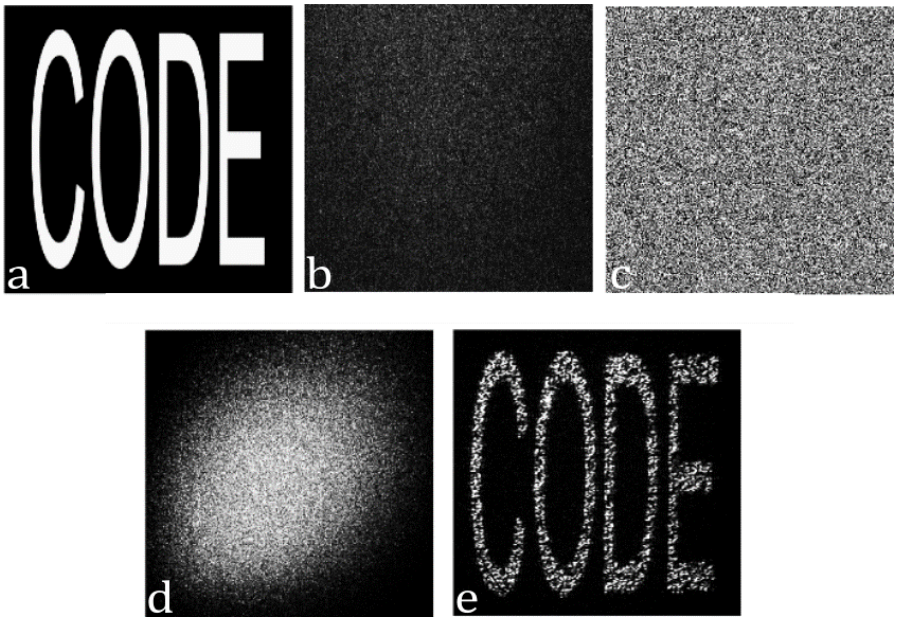

Figura 36: Resultados experimentales de encriptación con un FrJTCC. a) objeto de entrada, b) JFrPD, c) objeto encriptado, d) objeto desencriptado con llave incorrecta y e) objeto desencriptado correctamente.

En la Figura 36 se muestran resultados experimentales de encriptación con un FrJTCC. Tal y como se espera de un sistema DRPE, cuando se intenta desencriptar con la llave incorrecta, se obtiene un diagrama de ruido blanco (Figura 36.d), sin embargo, si se conoce la información de la llave y el orden fraccional se obtiene una desencriptación

satisfactoria (Figura 36.e). Este resultado se obtuvo usando distancias $d_1 = 180mm$, $d_2 = 250mm$ y $f = 200mm$, dando lugar a un orden fraccionario $\alpha = 1.57 - 0.14i$.

A continuación, probaremos el desempeño del sistema cuando se desencripta con la llave correcta y el orden fraccional incorrecto. Debido a que variar de forma continua el orden fraccional puede ser complejo experimentalmente, ya que depende de tres parámetros (d_1, d_2 y f, ver ecuación (2.5.3)), para llevar a cabo esta prueba solo cambiaremos la distancia lente cámara d_2, manteniendo las otras dos distancias fijas. Así, se tomó el objeto encriptado de la Figura 36.c y se desencriptó con la llave correcta y transformadas fraccionarias de Fourier inversas (TFrFI) correspondientes a distancias d_1 en un rango entre 244 y 256 mm. Luego se calculó el NMSE entre el objeto desencriptado con la distancia correcta y los obtenidos con las distancias incorrectas.

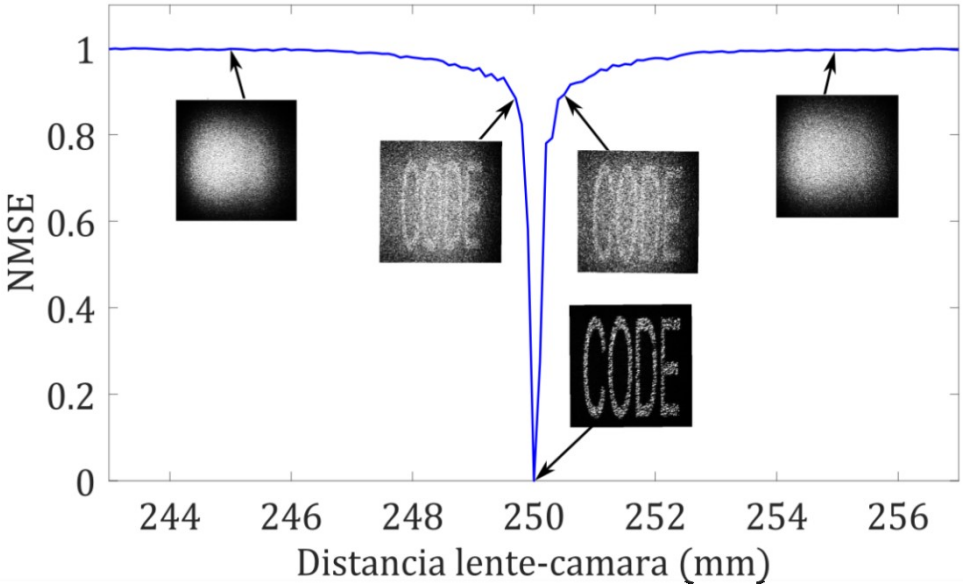

Figura 37: NMSE del objeto desencriptado con diferentes distancias lente-cámara.

En la Figura 37, se muestra el resultado de esta prueba. Se puede apreciar una degradación gradual del objeto desencriptado cuando la distancia lente-cámara cambia. Las imágenes insertadas, correspondientes a las distancias 245mm y 255mm, muestran que con este desplazamiento el objeto no puede ser reconocido satisfactoriamente. Como un cambio en la distancia lente-cámara representa un cambio en el orden fraccional, podemos concluir que el orden fraccional presenta una tolerancia que hace que este no sea un parámetro ideal de seguridad. Sin embargo, vale la pena señalar, que esta

tolerancia es menor que la de un JFSC, lo que hace al orden fraccional un parámetro más seguro que la distancia de propagación en el JFSC.

En lo descrito en las últimas dos secciones, vemos que no hay diferencias importantes en el desempeño de los sistemas DRPE cuando se implementan con otras transformaciones diferentes a la de Fourier. El motivo de esta similitud puede explicarse en el hecho de que tanto la transformada de Fourier, como la de Fresnel y la transformada Fraccionaria de Fourier tienen la propiedad de convolución y correlación, necesaria para permitir la correlación entre dos funciones aleatorias, que es la esencia del sistema DRPE.

2.6. Ataques.

Tras analizar el desempeño de sistemas DRPE implementados en distintos dominios, ahora procederemos a estudiar la seguridad de estos antes distintos ataques. En este caso, nos centraremos en estudiar el sistema DRPE en el dominio de Fourier, debido a que, como mostramos en las secciones anteriores, los principios básicos de funcionamiento no varían ni en el dominio de Fresnel ni en el fraccional. Aquí usaremos la terminología del criptoanálisis, refiriéndonos al objeto original como texto plano, y al objeto encriptado como texto cifrado.

En criptoanálisis, hay definidos tres tipos de ataques generales que se pueden intentar para vulnerar un sistema de encriptación, según el nivel de acceso que tiene el adversario al mismo. El primer tipo de ataque es el de texto plano elegido (CPA por las siglas en ingles de “chosen plaintext attack”). Son ataques de texto plano elegido aquellos en los cuales el adversario tiene acceso total al sistema de encriptación, y puede encriptar todos los objetos que quiera. La resistencia a este tipo de ataques hace que un sistema tenga “seguridad perfecta”. En la práctica, la gran mayoría de los sistemas de encriptación, tanto ópticos como tradicionales son vulnerables a los CPA.

El siguiente tipo de ataque es el ataque de texto plano conocido (KPA por las siglas en ingles de “known plaintext attack”). En los ataques de este tipo, el adversario conoce un número limitado de objetos encriptados y los objetos originales a los que corresponden. Con esta información, el adversario intenta deducir la llave de encriptación, para poder vulnerar otros objetos encriptados con el sistema.

El último tipo de ataque es llamado ataque de solo texto cifrado (COA por las siglas en ingles de “ciphertext only attack”). En este tipo de ataque el adversario intenta recuperar información del objeto original o de la llave solo conociendo el objeto encriptado. La vulnerabilidad a COA es considerada una falla critica en un sistema de encriptación.

A continuación, detallaremos algunos de estos tipos de ataques con el propósito de ilustrar algunas de las vulnerabilidades de la encriptación óptica para posteriormente presentar una técnica novedosa que ayuda a frustrar gran parte de los ataques conocidos.

2.6.1. Ataque de texto plano elegido.

El ataque de texto plano elegido fue el primero en ser demostrado contra el sistema DRPE [36]. Para explicar este tipo de ataque usaremos el criptosistema JTC de la sección 2.3, donde el objeto encriptado está dado por

$$E(v,w) = C(v,w)K^*(v,w) \tag{2.6.1}$$

Ahora supongamos que el objeto original es una función delta de Dirac, tal que $c(x,y) = \delta(x,y)r(x,y)$, donde $r(x,y)$ es la máscara de fase que multiplica al objeto. Realizando la TFI del objeto encriptado, obtenemos que

$$\begin{aligned} e(x,y) &= c(x,y) \otimes k(x,y) \\ e(x,y) &= \delta(x,y)r(x,y) \otimes k(x,y) \\ e(x,y) &= Rk(x,y) \end{aligned} \tag{2.6.2}$$

Donde R es el valor de la máscara de fase $r(x,y)$ en las coordenadas $(0,0)$. De la ecuación anterior, vemos que el resultado de la TFI de una delta de Dirac encriptada es igual a la llave de encriptación $k(x,y)$ multiplicada por un valor constate de fase. Así pues, el adversario puede recuperar directamente la llave con este procedimiento, con lo cual luego puede desencriptar cualquier otro objeto que sea encriptado con la misma llave.

Otra forma de lograr un CPA es encriptando una señal con una sola frecuencia espacial, por ejemplo, un coseno. Al hacer esto el objeto encriptado seria

$$E(v,w) = \frac{1}{2}\left[\delta(v-A,w) - \delta(v+A,w)\right]K^*(v,w) \tag{2.6.3}$$

Donde A es la frecuencia espacial de la señal. Este "objeto encriptado" es en realidad un muestreo de $K^*(v,w)$ en las coordenadas $(v \pm A, w)$. Encriptando señales con distintas frecuencias espaciales, el adversario puede ir muestreando pixel por pixel la llave, hasta finalmente obtenerla. Por supuesto, en un sistema de encriptación practico la llave rara vez tendrá menos de 100x100 pixeles, lo que implicaría que el adversario necesitaría encriptar 5000 señales para recuperar completamente la llave. Lamentablemente, los sistemas DRPE son tolerantes a la desencriptación con llaves parciales, lo cual facilita todos los tipos de ataque.

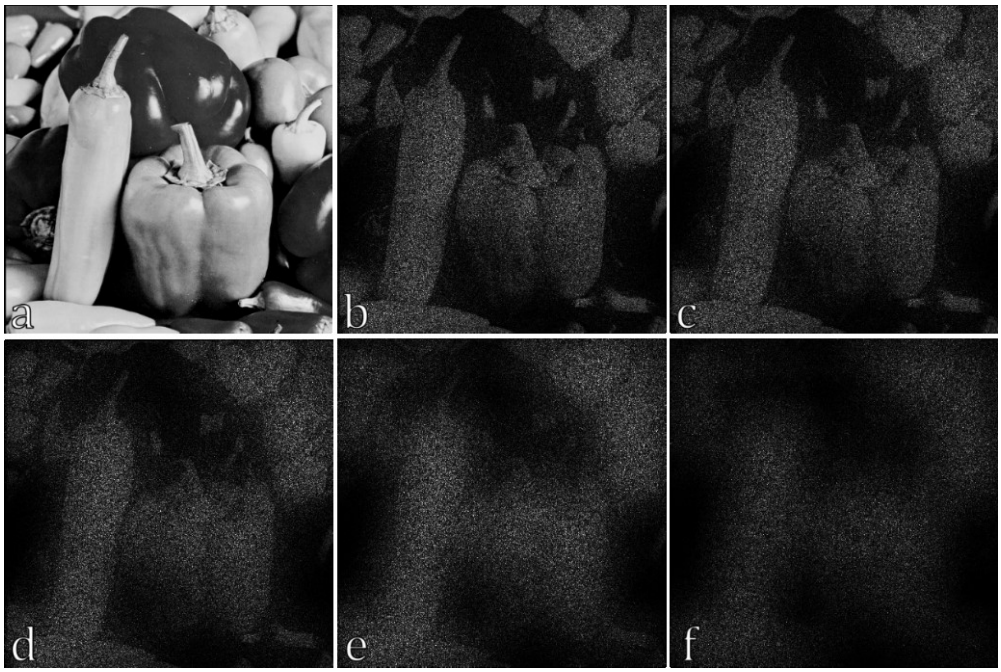

Figura 38: Resultados simulados de encriptación-desencriptación usando llaves parciales. A) objeto original, b) desencriptación con la llave completa de 100x100 pixeles, c) desencriptación con una sección de 80x80 pixeles de la llave, d) desencriptación con una sección de 60x60 pixeles de la llave, e) desencriptación con 40x40 pixeles de la llave y f) desencriptación con 20x20 pixeles de la llave.

En la Figura 38 se muestra el resultado de encriptar y desencriptar un objeto con un criptosistema JTC. La llave de encriptación usada tiene un tamaño de 100x100 pixeles. Desencriptando con una sección cuadrada de 80x80 pixeles de la llave, el objeto desencriptado es reconocible, aunque presenta deterioro respecto al objeto original. Al usar 60x60 pixeles este deterioro hace que los detalles finos del objeto se pierdan y con solo 40x40 pixeles el objeto desencriptado es prácticamente irreconocible.

Para realizar un análisis cuantitativo del efecto del uso de llaves parciales en la desencriptación, realizamos varias desencriptaciones con un porcentaje decreciente de

pixeles de la llave y calculamos el coeficiente de correlación entre el objeto original y los objetos desencriptados con las llaves parciales. El coeficiente de correlación está definido como

$$cc = \frac{\sum_{p,q}^{N,M} (A(p,q) - \bar{A})(B(p,q) - \bar{B})}{\sqrt{\left(\sum_{p,q}^{N,M} (A(p,q) - \bar{A})^2 \right) \left(\sum_{p,q}^{N,M} (B(p,q) - \bar{B})^2 \right)}} \tag{2.6.4}$$

Donde A y B son las imágenes a correlacionar, $\bar{A}$ y $\bar{B}$ sus promedios y (p,q) son coordenadas de pixel.

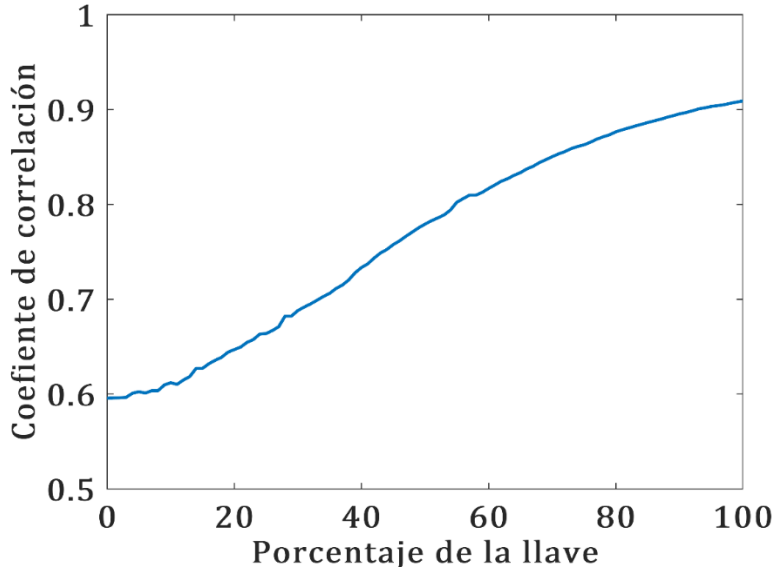

Figura 39: Coeficiente de correlación entre el objeto original y el objeto desencriptado con llaves parciales.

Como se observa en la gráfica, el coeficiente de correlación se reduce de forma proporcional al porcentaje de la llave que se conoce a la hora de desencriptar. En este resultado debe tenerse en cuenta que no existe un valor del coeficiente de correlación que permita aseverar que ninguna información sobre el objeto es reconocible, ya que la identificación de la información en el objeto desencriptado, sobre todo cuando este es una imagen, depende de las características del objeto original y de factores subjetivos propios de la percepción humana.

Debido a la tolerancia a la desencriptación con llaves parciales, en el ejemplo de la Figura 38, un adversario que intente aplicar CPA por medio de encriptación de señales periódicas necesitara en vez de 5000 encriptaciones para hallar una llave de 100x100

pixeles, tan solo 1800, con las cuales conseguiría muestrear una sección de 60x60 pixeles, la cual es suficientes para identificar el objeto encriptado. La degradación causada por usar llaves parciales tiene características similares a un filtro paso bajo o gaussiano, es decir, que las altas frecuencias del objeto encriptado son las primeras en verse afectadas. Así pues, un objeto simple con pocos detalles podrá identificarse con pocos pixeles de la llave, y uno complejo requerirá un porcentaje mayor.

Aunque lo descrito anteriormente parece pintar un paisaje desalentador sobre la seguridad de los sistemas DRPE, tengamos en cuenta que los dos CPA expuestos hasta ahora se basan en la consideración de un sistema ideal. En un sistema óptico real su realización es improbable en el mejor de los casos, y proteger el sistema contra los mismo resulta casi trivial.

En el ataque por delta de Dirac, recordemos que solo se puede usar una aproximación de esta función, ya que es una distribución matemática. En la práctica, el ataque implicaría encriptar una apertura lo más pequeña posible. La capacidad del ataque para obtener la llave se ve gravemente afectada por usar una pupila con tamaño finito en vez de una delta de Dirac. Así pues, para impedir este tipo de ataque bastaría con imponer un tamaño mínimo a los objetos a ser encriptados.

El ataque por señales periódicas implica que se encripta una función coseno o un seno. Sin embargo, estas funciones tienen extensión infinita, lo no se puede lograr en un sistema óptico. La precisión de las muestras de la llave obtenidas en cada encriptación va a disminuir rápidamente conforme se limite la extensión de la señal. Análogamente al ataque delta de Dirac, la forma más sencilla de asegurar el sistema contra este ataque es imponer un máximo al tamaño del objeto, lo cual en la mayoría de los casos no será necesario, pues los sistemas experimentales normalmente están limitados a procesar objetos relativamente pequeños.

2.6.2. Ataques de texto plano conocido.

Existe una gran variedad posible de KPA, dependiendo del número de pares texto cifrado-texto plano de los que dispone el adversario. El tipo más general es el KPA con solo un texto plano y su correspondiente texto cifrado, propuesto por primera vez por Xiang *et al* [37]. Sea el texto cifrado dado por

$$E(v,w) = \left[O(v,w) \otimes R(v,w)\right] K^{*}(v,w) \tag{2.6.5}$$

Donde $O(v,w)$ es la TF del texto plano, y $R(v,w)$, $K(v,w)$ son las TF de la máscara de fase que multiplica al texto plano y la llave respectivamente. Elevando el texto cifrado anterior al cuadrado obtenemos que

$$|E(v,w)|^2 = \left|\left[O(v,w) \otimes R(v,w)\right] K(v,w)\right|^2 \qquad (2.6.6)$$

Este ataque supone que $K(v,w)$ es una función de fase pura, por lo que $|K(v,w)|^2 = 1$. Así obtenemos que

$$|E(v,w)|^2 = \left|\left[O(v,w) \otimes R(v,w)\right]\right|^2 \qquad (2.6.7)$$

La ecuación (2.6.7) indica que la intensidad del objeto encriptado es igual a la intensidad de la transformada de Fourier del texto plano multiplicado por la máscara de fase correspondiente. Con esta información, el adversario puede deducir la máscara de fase $r(x,y)$ que multiplica al objeto, aplicando un algoritmo de reconstrucción de fase.

Un algoritmo de reconstrucción de fase es un método iterativo que permite, a partir de la intensidad de un campo óptico o señal en el plano de entrada y su plano de Fourier, reconstruir la fase faltante. El primer algoritmo de este tipo fue propuesto por R. W Gerchberg y W. O. Saxton [38], por lo que comúnmente es conocido como el algoritmo de Gerchberg-Saxton (G-S).

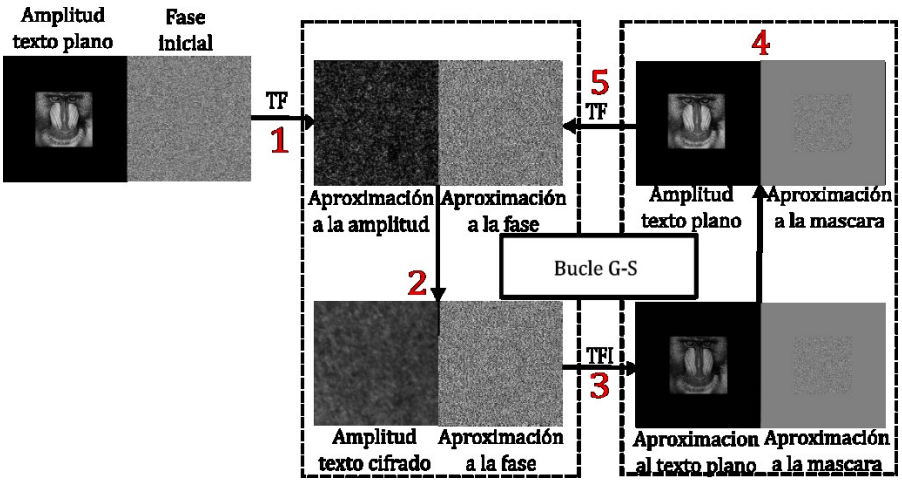

Figura 40: Algoritmo G-S para obtener la máscara de fase.

Este algoritmo consiste en el siguiente proceso, ilustrado en la Figura 40. Sea la máscara que multiplica el texto plano dada por $r(x,y) = e^{i\theta(x,y)}$ donde $\theta(x,y)$ es una función aleatoria con valores unifórmeme distribuidos entre 0 y 2π, $o(x,y)$ el texto

plano, $E(v,w)$ el texto cifrado, y $F_k(v,w)$, $\phi_k(x,y)$ y $o_k(x,y)$ estimaciones de $E(v,w)$, $\theta(x,y)$ y $o(x,y)$ respectivamente tras k iteraciones del algoritmo G-S.

1. Se multiplica el texto plano por la estimación de la máscara de fase, que en la primera iteración es una función aleatoria cualquiera y se realiza la transformada de Fourier, obteniendo

$$F_k(v,w) = |F_k(v,w)| e^{i\phi'_k(v,w)} = TF\left\{o(x,y)e^{i\phi_k(x,y)}\right\} \quad (2.6.8)$$

   Donde la fase de $F_k(v,w)$ la definimos como $\phi'_k(v,w)$.

2. Se reemplaza la amplitud de $F_k(v,w)$ por la amplitud del texto cifrado, tal que

$$F'_k(v,w) = |E(v,w)| e^{i\phi'_k(v,w)} \quad (2.6.9)$$

3. Se realiza la transformada de Fourier inversa (TFI) del campo obtenido en 2, obteniendo

$$o_k(x,y) = |o_k(x,y)| e^{i\theta_k(x,y)} \quad (2.6.10)$$

4. Se reemplaza la amplitud de la TFI obtenida en 3 por la amplitud del texto plano.

$$o'_k(x,y) = |o(x,y)| e^{i\theta_k(x,y)} \quad (2.6.11)$$

5. Se realiza la TF del campo obtenido en 4.

Este proceso se repite hasta que la amplitud aproximada que se obtiene en 3 sea lo más similar posible a la amplitud del texto plano. Una vez se cumple esta condición, la fase que acompaña a esta amplitud corresponde de manera aproximada a la máscara de fase $r(x,y)$.

Una vez el adversario conoce la máscara $r(x,y)$, puede hallar el complejo conjugado de la TF de la llave $K^*(v,w)$ si realiza la TF del producto de $r(x,y)$ por el texto plano, y luego divide el texto cifrado por el resultado, tal que

$$K^*(v,w) = \frac{E(v,w)}{O(v,w) \otimes R(v,w)} \quad (2.6.12)$$

Una vez el adversario tiene $K^*(v,w)$, ha logrado su cometido y puede desencriptar cualquier texto cifrado con el mismo par de máscaras.

Este ataque requiere de dos supuestos importantes para ser efectivo. El primero es que $|K(v,w)|^2=1$. Este supuesto se cumple en general para los sistemas 4f, ya que la máscara de fase que corresponde a la llave está ubicada en el plano de Fourier del objeto, sin embargo, en el caso del criptosistema JTC, esta máscara está ubicada en el mismo plano que el objeto, y aunque la máscara sea de fase pura, su transformada de Fourier no necesariamente lo será. Esto implica que el uso de este ataque para un sistema JTC requiere de algunas modificaciones. En particular, la gran mayoría de los KPA aplicados a los sistemas JTC parten del supuesto de que el texto cifrado es el JPS, y su implementación se hace casi imposible si se filtra el JPS para obtener el texto cifrado en la forma de la ecuación (2.6.5) [39].

La otra suposición que requiere este ataque es que el texto plano sea información solo de amplitud. La presencia de información de fase en el objeto causa una alteración en la fase recuperada con el algoritmo de G-S, ya que ésta no corresponderá únicamente a $r(x,y)$.

Por otro lado, el resultado del algoritmo G-S es solo una aproximación al valor real de $r(x,y)$ y por lo tanto así también lo será la llave obtenida con este ataque. Como se describió en la subsección anterior, los sistemas DRPE tienen la característica de permitir la desencriptación con llaves aproximadas, aunque con degradación respecto a la desencriptación con la llave correcta. En este sentido, los objetos desencriptados con las llaves obtenidas con el KPA aquí descrito presentaran un grado significativo de deterioro, lo cual hace este tipo de ataque poco útil para violentar sistemas que procesen textos planos en escala de grises o con un elevado nivel de detalle.

Por último, ya hay en la literatura varias propuestas para hacer a los sistemas DRPE resistentes a este ataque. La más simple de estas propuestas consiste en dividir el texto cifrado por su amplitud [40]. De esta manera, el nuevo texto cifrado solo tendría información de fase, y no se podría aplicar el algoritmo G-S. Este método se sustenta en que la fase una señal es suficiente para su reconstrucción, tal y como expusimos en la sección 1.8.

2.6.3. Ataques de solo texto cifrado.

Los ataques COA fueron los últimos en ser demostrados en contra de los sistemas DRPE, debido a la complejidad de estos. Estos ataques operan con un planteamiento muy similar

al del KPA descrito en la subsección anterior. El adversario, conociendo el texto cifrado, puede obtener la intensidad de la TF de texto plano multiplicada por la máscara de fase, como se muestra en la ecuación (2.6.7), sin embargo al no disponer del texto plano, no se puede aplicar directamente el algoritmo de G-S para recuperar la información de la llave.

Afortunadamente para el adversario, este tipo de problema, en el cual se trata de reconstruir un objeto a partir de la amplitud de su transformada de Fourier ha sido ampliamente estudiado, debido a su importancia en aplicaciones de cristalografía y visión a través de medios difusos. En particular, James Fineup [41] encontró que si se establecen algunas condiciones sobre el objeto, es posible reconstruirlo a partir de la amplitud de su TF.

Estas restricciones implican que el objeto tiene que ser real y positivo, lo cual en un sistema DRPE implica que tiene que ser un objeto de solo amplitud. Adicionalmente, para garantizar una solución efectiva, se requiere alguna información sobre el objeto, como por ejemplo su "soporte". El soporte de un objeto es su extensión en el plano de entrada. Es decir, si nuestro objeto es una imagen de 100x100 pixeles, su soporte será un cuadrado de 100x100 pixeles.

El algoritmo original presentado por Fineup, llamado algoritmo de corrección de errores (algoritmo EC por las siglas en ingles de "error correction") es una generalización del algoritmo G-S. Los primeros COA reportados en la literatura se basan en el supuesto de que el adversario conoce el soporte del texto plano [42]. Partiendo de ese supuesto, el COA por medio del algoritmo de reconstrucción de fase EC procede como se describe a continuación.

1. El adversario comienza con un estimativo del objeto, el cual definiremos como $o_k(x,y)$. Este estimativo puede ser el soporte del objeto. Sea $\phi_k(x,y)$ una fase estimada del objeto, la cual puede ser cualquier función aleatoria, entonces

$$o_k(x,y) = |\, o_k(x,y) \,| \, e^{i\phi_k(x,y)} \tag{2.6.13}$$

2. El adversario realiza la TF $o_k(x,y)$, obteniendo

$$F_k(v,w) = |\, F_k(v,w) \,| \, e^{i\phi'_k(v,w)} \tag{2.6.14}$$

3. Se reemplaza la amplitud de $F_k(v,w)$ por la amplitud del texto cifrado, conservando la fase, tal que

$$F'_k(v,w) = |E(v,w)|\, e^{i\phi'_k(v,w)} \tag{2.6.15}$$

4. Se realiza la TFI de $F'_k(v,w)$, obteniendo un nuevo estimativo del objeto $o'_{k+1}(v,w)$

5. Se aplican las ligaduras teniendo en cuenta lo que se conoce del objeto. Definiendo γ como el dominio en el cual $o'_{k+1}(x,y)$ es positivo, real y está dentro del soporte del objeto, el adversario obtiene una nueva estimación del objeto tal que

$$o_{k+1}(x,y) = \begin{cases} o'_{k+1}(x,y) & (x,y) \in \gamma \\ 0 & (x,y) \notin \gamma \end{cases} \tag{2.6.16}$$

Este proceso se repite hasta que $|F(v,w)|$ sea lo más aproximado posible a $|E(v,w)|$ y $o_k(x,y)$ cumpla la ecuación (2.6.16). Si se cumplen estas condiciones, $o_k(x,y)$ será una buena aproximación al texto plano, permitiendo al adversario adquirir la información encriptada sin necesidad adquirir las llaves de encriptación.

La mayoría de los COA siguen una estrategia similar a la descrita anteriormente, y se diferencian principalmente en las ligaduras que usa el adversario a la hora de aplicar el algoritmo de reconstrucción de fase. Estas ligaduras pueden ser, adicionalmente al soporte del texto plano, el número de pixeles distintos de cero que compone el objeto [43]. Al igual que en los ataques KPA, una forma de dificultar este tipo de ataque en los sistemas JTC consiste en filtrar el JPS, ya que analizando los distintos órdenes que se encuentran en la TFI del JPS, es posible determinar el soporte y la geometría del plano de entrada, facilitando así el COA.

Aunque la vulnerabilidad a los ataques COA fue demostrada con simulaciones numéricas, mostrando buen rendimiento, la implementación experimental de los mismos ha demostrado que los COA con reconstrucción de fase solo son capaces de recuperar datos relativamente simples, como textos planos binarios [44,45]. Esto tiene dos motivos principales. Primero, el hecho de que, debido a las limitaciones en tamaño de pixel y resolución del medio de registro, en un sistema experimental el objeto encriptado es solo un muestreo parcial del objeto encriptado completo, lo cual dificulta la convergencia de los algoritmos de reconstrucción de fase. Segundo, los difusores que se usan en los

sistemas experimentales, no corresponden a máscaras de fase ideales, e introducen cambios aleatorios tanto en la fase de la luz como en su amplitud. Para evitar esta dificultad, los COA experimentales usan una estrategia ligeramente distinta, que fue originalmente concebida para la visualización óptica a través de medios difusos [46].

Sea el texto cifrado dado por la ecuación (2.6.5), su TFI está dada por

$$e(x,y) = o(x,y)r(x,y) \otimes k^*(x,y) \tag{2.6.17}$$

Donde esta vez, $k^*(x,y)$ es una función aleatoria tanto en amplitud como en fase. Si realizamos la autocorrelación del resultado anterior, obtenemos

$$\begin{aligned} e(x,y) \odot \quad & \odot \\ & \left[o(x,y)r(x,y) \otimes k^*(x,y) \right] \\ & = \left[o(x,y)r(x,y) \odot \quad (x,y) \right] \otimes \\ & \left[k^*(x,y) \odot \quad \right] \end{aligned} \tag{2.6.18}$$

Donde $\odot$ denota la operación de autocorrelación y $\otimes$ la de convolución. Como $k^*(x,y)$ es una función aleatoria en fase y amplitud, podemos aplicar la aproximación de ruido blanco de gran ancho de banda [22], tal que $k^*(x,y) \odot \quad \approx \delta(x,y)$. De esta manera

$$e(x,y) \odot \quad \odot \tag{2.6.19}$$

realizando la transformada de Fourier de la ecuación anterior y aplicando el teorema de la convolución, finalmente obtenemos

$$|E(v,w)|^2 \approx |O(v,w) \otimes R(v,w)|^2 \tag{2.6.20}$$

La intensidad aquí obtenida es solo una aproximación a la intensidad real de la TF del producto del objeto con la máscara de Fase, con una pérdida importante en las frecuencias altas, pero es suficiente para permitir recuperar la información de textos planos simples usando un algoritmo de reconstrucción de fase si se conoce el soporte del objeto.

Tanto el KPA como el COA aquí descritos pueden adaptarse a los criptosistemas fraccionales y de Fresnel, usando algoritmos iterativos modificados para operar en esos dominios [47].

2.6.4. Salteado criptográfico en sistemas DRPE

La demostración de los ataques descritos anteriormente estimularon la investigación en métodos para aumentar la seguridad de los sistemas ópticos de encriptación [48–50]. Aunque gran parte de esta investigación se ha centrado en modificaciones a los sistemas ópticos, una fuente de inspiración para resolver las vulnerabilidades de éstos consiste en estudiar los métodos de encriptación digitales. Entre las estrategias ampliamente usadas en estos métodos, encontramos el concepto de "salteado" criptográfico. El salteado criptográfico consiste en añadir datos aleatorios (llamados "sal") a un texto cifrado antes o después de la encriptación, de manera que aunque se encripte dos veces el mismo texto plano con la misma llave, el texto cifrado resultante será diferente [51].

El concepto de salteado cobra relevancia cuando se comenzaron a crear bases de datos que contenían las contraseñas encriptadas de miles, o cientos de miles de usuarios, con el propósito de permitir acceso seguro a información a través de internet. Rápidamente, se encontró que estas bases de datos podían ser vulneradas fácilmente con un análisis de entropía, en el cual el adversario simplemente comparaba la frecuencia con la que se repetía un determinado texto cifrado con la frecuencia con la que los seres humanos escogen ciertas expresiones como contraseña. De esta manera, es posible suponer una porción de los textos planos correspondientes a la base de datos, y luego realizar un KPA para encontrar la llave de encriptación de los demás textos cifrados.

Teniendo en cuenta lo anterior, Velez *et al* [52] proponen extender el concepto de salteado a los sistemas ópticos. Para esto, se propone multiplexar el texto cifrado que contiene la información a proteger con otro texto cifrado correspondiente a una "sal". La sal se cambia cada vez que se encripte un texto plano, garantizando que dos textos cifrados sean siempre distintos aun cuando se encriptan con la misma llave.

Así el texto cifrado salteado será dado por

$$E_s(v,w) = [O(v,w) \otimes R(v,w)]K^*(v,w) + [S(v,w) \otimes R(v,w)]K^*(v,w) \tag{2.6.21}$$

Donde $O(v,w)$, $S(v,w)$, $R(v,w)$ y $K^*(v,w)$ son las TFs del objeto $o(x,y)$, la sal $s(x,y)$, la máscara de fase $r(x,y)$ y el complejo conjugado de la llave $k(x,y)$. Tras desencriptar correctamente, se obtiene

$$d_s(x,y) = [o(x,y)r(x,y)] + [s(x,y)r(x,y)] \qquad (2.6.22)$$

lo que corresponde a una superposición entre el objeto desencriptado y la sal. Para efectos de esta propuesta, suponemos que un usuario autorizado tiene acceso tanto a las máscaras de fase como al texto plano de la sal. De esta manera, el usuario puede sustraer la sal de la ecuación (2.6.22), obteniendo el texto plano de interés sin degradación debido a su superposición con la sal. Por otro lado, el texto cifrado correspondiente a la sal no debe estar disponible para nadie, ya que el disponer de esta información hace trivial el deshacer el proceso de salteado.

Para probar experimentalmente la viabilidad de nuestra propuesta, usamos un criptosistema JTC como el descrito en la sección 2.3, con un tamaño del objeto y de la ventana de la llave de $4.096\,mm \times 4.096\,mm$. El modulador es un Holoeye LC-2002 con resolución de 800x600 pixeles y tamaño de pixel de $32\,\mu m \times 32\,\mu m$. Un láser de estado sólido bombeado por diodo de $300\,mW$ de potencia y longitud de onda de $532\,nm$ sirvió de fuente de iluminación y la lente del sistema era de $200\ mm$ de distancia focal. Como medio de registro usamos una cámara CMOS EO-10012C de 3840×2748 pixeles de resolución y tamaño de pixel de $1.67\,\mu m \times 1.67\,\mu m$.

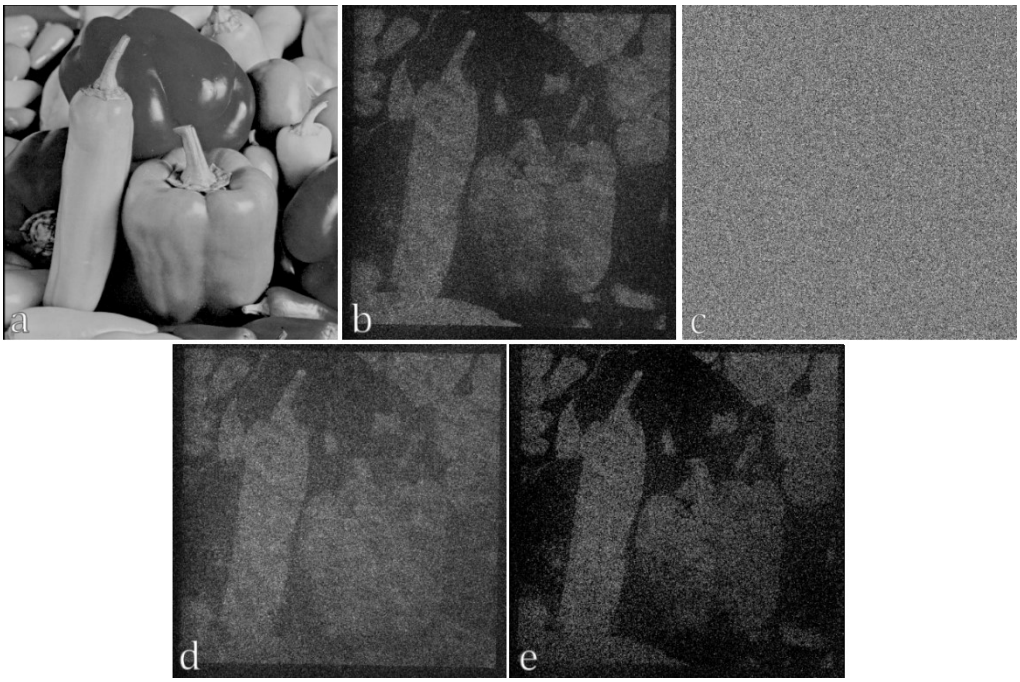

Figura 41: Datos desencriptados de un texto cifrado salteado: a) Texto plano, b) texto plano desencriptado a partir de un texto cifrado sin salteado, c) texto plano de la sal, d) texto plano desencriptado a partir del texto cifrado salteado, y e) resultado obtenido tras sustraer el texto plano de la sal de d).

En la Figura 41, se muestran los resultados de encriptar y desencriptar un texto plano (Figura 41.a) sin y con salteado (Figura 41.b y d respectivamente). Como sal elegimos una máscara de amplitud aleatoria (Figura 41.c). Como podemos apreciar de estos resultados, el texto cifrado salteado presenta degradación respecto al resultado sin salteado, sin embargo, la información del texto plano original es reconocible. Debido a esta característica, el salteado por sí mismo no se comporta como una nueva llave de encriptación o parámetro de seguridad. Adicionalmente, en la Figura 41.e podemos constatar que al sustraer el texto plano de la sal, se elimina gran parte de la degradación causada por la superposición con la sal.

Ahora procederemos a estudiar el efecto del salteado en los distintos ataques descritos en las subsecciones anteriores, empezado por el ataque de delta de Dirac. Si intentamos encriptar una delta de Dirac con un sistema que realice salteado, tras realizar la TFI del texto cifrado resultante obtenemos

$$\begin{aligned} e_{scpa}(x,y) = &[\delta(x,y)r(x,y)] \otimes k^*(x,y) \\ &+[s(x,y)r(x,y)] \otimes k^*(x,y) \end{aligned} \tag{2.6.23}$$

En esta expresión, la información del complejo conjugado de la llave $k(x,y)$ que se obtiene con el ataque delta de Dirac esta superpuesta con la TFI del texto cifrado de la sal. Esta superposición evita que el adversario pueda obtener la llave correctamente, siempre y cuando la sal tenga un soporte igual o mayor al tamaño de la llave. Debido a que el sistema experimental no permite realizar un ataque de delta de Dirac ideal, para confirmar la capacidad del salteado de hacer resistente el cryptosistema ante este ataque, usamos un sistema simulado con los mismos parametros opticos, objeto de entrada y sal que con los que se obtuvieron los resultados experimentales.

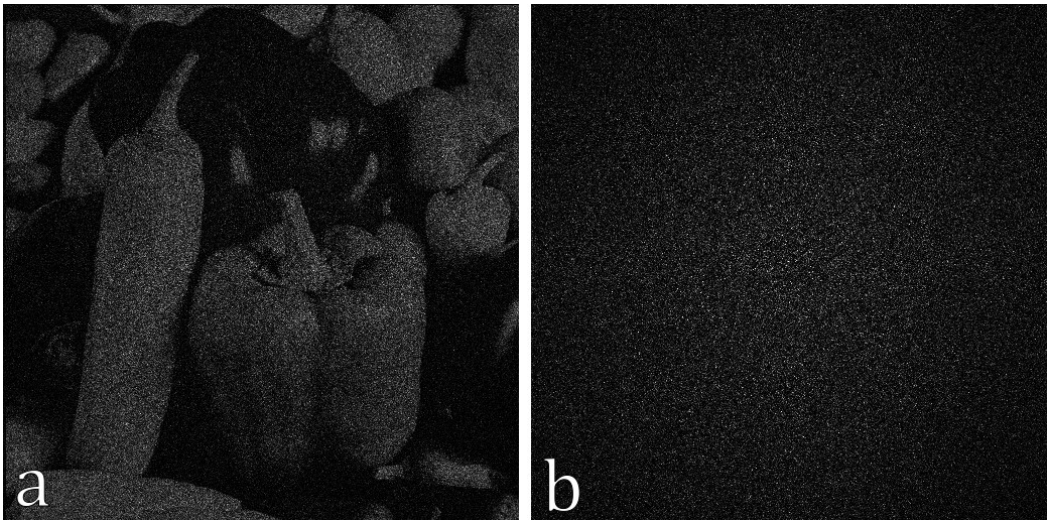

Figura 42: Objetos desencriptados con la información obtenida tras un ataque delta de Dirac: a) en un sistema sin salteado, b) en un sistema con salteado.

El resultado de esta prueba se muestra en la Figura 42. Como podemos verificar a partir de la ecuación (2.6.23), el resultado del ataque de delta de Dirac en un sistema con salteado no permite obtener ninguna información al intentar desencriptar el texto cifrado (Figura 42.a), a diferencia de lo que ocurre en un sistema sin salteado, en el cual la llave se recupera totalmente, permitiendo la desencriptación (Figura 42.b).

Ahora procederemos a probar la resistencia a los KPA del texto cifrado salteado. El KPA se basa en el hecho de que la intensidad del texto cifrado es igual a la intensidad de la TF del texto plano multiplicado por la máscara de fase, como se muestra en la ecuación (2.6.7), lo que permite encontrar la fase usando el algoritmo de G-S. Esta igualdad no se mantiene cuando se realiza el salteado, ya que la intensidad del texto cifrado salteado es dada por

$$\begin{aligned} |E_s(v,w)|^2 = & |O(v,w)\otimes R(v,w)|^2 + |S(v,w)\otimes R(v,w)|^2 \\ & +[S(v,w)\otimes R(v,w)]^* \times [O(v,w)\otimes R(v,w)] \\ & +[S(v,w)\otimes R(v,w)]\otimes [O(v,w)\otimes R(v,w)]^* \end{aligned} \qquad (2.6.24)$$

Debido a la presencia de varios órdenes adicionales que surjan del salteado, el resultado de aplicar el algoritmo de G-S con el texto cifrado salteado y el texto plano del objeto no corresponderá a la máscara $r(x,y)$, y no podrá usarse para extraer la información de la llave $k(x,y)$.

Debido a lo anterior, el COA también se ve frustrado. A continuación, intentaremos aplicar el COA. Para ello, primero encriptaremos un objeto simple usando el criptosistema

simulado, con y sin salteado, y luego trataremos de reconstruirlo aplicando el algoritmo de reconstrucción de fase HC a la autocorrelación de la TF de los textos cifrados, suponiendo que conocemos tanto el soporte como el número de pixeles no nulos del texto plano.

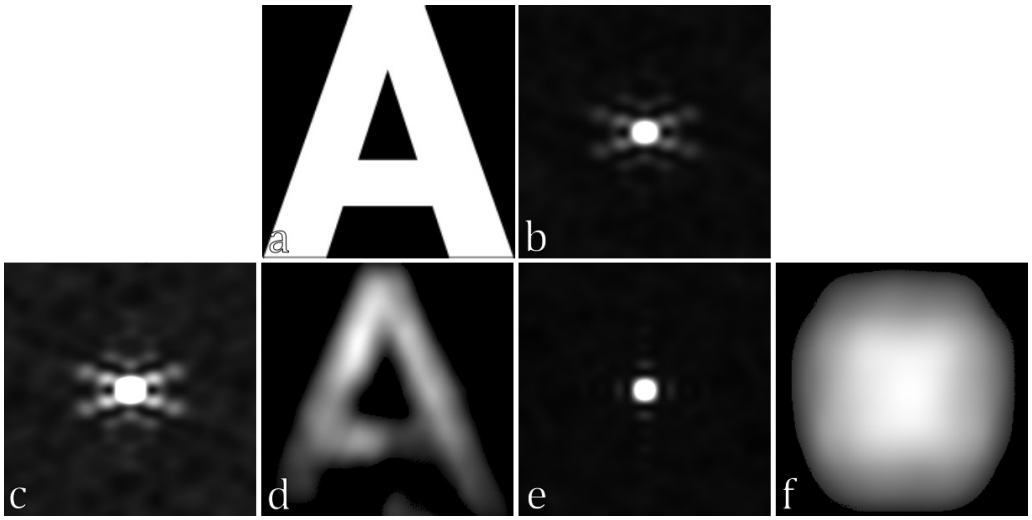

Figura 43: Resultado de COA en un sistema JTC simulado. a) texto plano, b) autocorrelación texto plano, c) autocorrelación texto cifrado, d) texto plano reconstruido con COA a partir de c), e) autocorrelación texto cifrado salteado, y f) texto plano recuperado con COA a partir de e).

En la Figura 43 se muestra el resultado de intentar el COA. En este caso la sal usada fue una máscara aleatoria de amplitud. En el caso sin salteado, el COA permite recuperar el texto plano (Figura 43.d). Como podemos observar, la autocorrelación del texto plano (Figura 43.b) y del texto cifrado (Figura 43.c) tienen un alto grado de similitud. Esta característica es lo que hace vulnerable los sistemas DRPE a ataques KPA y COA. Por otro lado, la autocorrelación del texto cifrado salteado (Figura 43.e) no se asemeja a la del texto plano, haciendo imposible la recuperación del texto plano a partir de la misma (Figura 43.f).

2.7. Contenedores de información.

Tras la presentación en la sección anterior sobre la seguridad de los sistemas DRPE, ahora nos centraremos en estudiar otra de las características que ha limitado sus aplicaciones: la degradación de los datos desencriptados a partir de un texto cifrado con DRPE. Como hemos podido comprobar, tanto en los resultados experimentales como en los simulados, esta degradación se manifiesta en forma de ruido de speckle, el cual puede afectar seriamente la capacidad de reconocer el objeto desencriptado.

La investigación sobre este problema se dividió en dos estrategias, que han dado lugar a importantes avances en seguridad óptica. La primera, basada en la hipótesis de que el ruido en los sistemas DRPE es debido a las limitaciones propias de sus implementaciones experimentales, y la segunda en la cual se intentó entender las causas del ruido a partir de estudios teóricos y simulados.

Siguiendo el primer planteamiento, la investigación se centró en buscar estrategias para que el ruido no sea una limitación en las aplicaciones de los sistemas DRPE. Entre estas estrategias encontramos el uso del multiplexado para encriptar datos cuya longitud o nivel de detalle supere los limites prácticos del sistema, por ejemplo, dividiendo una imagen a encriptar en secciones más pequeñas, encriptándolas y luego multiplexando de forma que al desencriptar el paquete se recupere el objeto con una calidad superior [53], o bien el uso de teclados encriptados para codificar mensajes extensos [54], entre otros.

Es en este contexto que Barrera *et al* proponen el uso de "contenedores" de información para facilitar el procesamiento de datos con métodos ópticos [55,56]. La idea detrás de este concepto es el transformar la información a ser encriptada en una representación (contenedor) menos susceptible al ruido de speckle, procesarla con el sistema óptico, y luego realizar la transformación inversa sobre el resultado para recuperar la información original, libre de ruido.

El contendor elegido por los autores fue el código de respuesta rápida (QR por las siglas en ingles de "quick response"). El código QR es un código binario inventado por Denso Wave en 1994 para hacer seguimiento a las partes de un vehículo durante su manufactura, pero ha adquirido un uso generalizado en muchas aplicaciones, debido a que puede ser leído fácilmente usando la cámara de un teléfono celular. Los códigos QR hacen uso del algoritmo de corrección de errores de Solomon-Reed [57], permitiendo así que la información que contienen pueda ser leída aun si parte del código se pierde. Esto los hace buenos candidatos como contenedores, ya que al encriptar un código QR, y posteriormente desencriptarlo, es posible leer el resultado, aunque sea afectado por ruido.

A pesar de estas características, el código QR no es necesariamente un contenedor ideal para los sistemas ópticos, ya que su diseño es optimizado para ser resistente a daño localizado, como por ejemplo si un código impreso sufre de un corte accidental, mientras que el ruido introducido por el DRPE afecta casi uniformemente el objeto desencriptado.

Esto plantea la pregunta ¿Qué características debe tener un contenedor ideal para ser usado en sistemas ópticos? Para responder a esta pregunta planteamos los siguientes criterios. a) el contenedor debe tener frecuencias espaciales bajas para minimizar las perdidas por difracción y el tamaño de pixel necesario en el medio de registro, b) el contenedor debe tener un nivel de tolerancia al ruido controlable, de manera que se pueda garantizar lectura óptica sin ser ineficiente, y c) el contenedor debe ser legible de forma rápida y sencilla.

Siguiendo este razonamiento, presentamos en la Figura 44 el primer contenedor de información específicamente diseñado para su uso en sistemas ópticos de seguridad como el DRPE el cual llamaremos contenedor diseñado para la seguridad óptica (CCOS por las siglas en ingles de "customized container for optical security") [58]. A continuación, describiremos este código y compararemos su desempeño con los códigos QR cuando son usados en un criptosistema JTC.

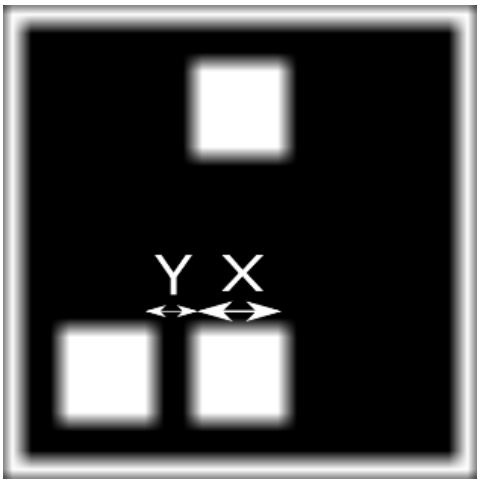

Figura 44: Contenedor de información propuesto para el carácter "C". X es el tamaño de bloque y Y la separación entre los bloques.

El CCOS básico es un arreglo binario cuadrado de 3x3 celdas, en el cual cada celda contiene un bloque de tamaño X, con una separación Y entre los bloques. El arreglo está rodeado de un borde blanco que delimita el código. La lectura del código se realiza de la siguiente manera: la intensidad promedio de cada celda se calcula de izquierda a derecha y de arriba abajo y luego es comparada con un valor limite que depende del sistema óptico (en nuestro caso, el valor limite es el 70% de la intensidad máxima del resultado de desencriptar un texto cifrado con el sistema JTC). Si la celda tiene una intensidad promedio por encima del valor límite se le asigna un valor de 1, y de lo contrario de 0. Combinando los valores resultantes se obtiene un numero binario de 9 bits. En las

demostraciones subsiguientes, usaremos solo los primeros 8 bits contendidos en el código, ignorando el ultimo, que corresponde a la celda de la esquina derecha inferior. Estos 8 bits corresponden a un carácter usando el estándar ASCII (ver Tabla 1).

Tabla 1: Estándar ASCII extendido

0	0	(caracter nulo)	40	101000	(	80	1010000	P	120	1111000	x	160	10100000	á	200	11001000	╚	240	11110000	≡
1	1	☺	41	101001	)	81	1010001	Q	121	1111001	y	161	10100001	í	201	11001001	╔	241	11110001	±
2	10	☻	42	101010	*	82	1010010	R	122	1111010	z	162	10100010	ó	202	11001010	╩	242	11110010	≥
3	11	♥	43	101011	+	83	1010011	S	123	1111011	{	163	10100011	ú	203	11001011	╦	243	11110011	≤
4	100	♦	44	101100	,	84	1010100	T	124	1111100	|	164	10100100	ñ	204	11001100	╠	244	11110100	⌠
5	101	♣	45	101101	-	85	1010101	U	125	1111101	}	165	10100101	Ñ	205	11001101	═	245	11110101	⌡
6	110	♠	46	101110	.	86	1010110	V	126	1111110	~	166	10100110	ª	206	11001110	╬	246	11110110	÷
7	111	•	47	101111	/	87	1010111	W	127	1111111	⌂	167	10100111	º	207	11001111	╧	247	11110111	≈
8	1000	◘	48	110000	0	88	1011000	X	128	10000000	Ç	168	10101000	¿	208	11010000	╨	248	11111000	°
9	1001	○	49	110001	1	89	1011001	Y	129	10000001	ò	169	10101001	⌐	209	11010001	╤	249	11111001	∙
10	1010	◙	50	110010	2	90	1011010	Z	130	10000010	é	170	10101010	¬	210	11010010	╥	250	11111010	·
11	1011	♂	51	110011	3	91	1011011	[	131	10000011	â	171	10101011	½	211	11010011	╙	251	11111011	√
12	1100	♀	52	110100	4	92	1011100	\	132	10000100	ä	172	10101100	¼	212	11010100	╘	252	11111100	ⁿ
13	1101	♪	53	110101	5	93	1011101	]	133	10000101	à	173	10101101	¡	213	11010101	╒	253	11111101	²
14	1110	♫	54	110110	6	94	1011110	^	134	10000110	å	174	10101110	«	214	11010110	╓	254	11111110	■
15	1111	☼	55	110111	7	95	1011111	_	135	10000111	ç	175	10101111	»	215	11010111	╫	255	11111111	(DEL)
16	10000	►	56	111000	8	96	1100000	`	136	10001000	ê	176	10110000	░	216	11011000	╪			
17	10001	◄	57	111001	9	97	1100001	a	137	10001001	ë	177	10110001	▒	217	11011001	┘			
18	10010	↕	58	111010	:	98	1100010	b	138	10001010	è	178	10110010	▓	218	11011010	┌			
19	10011	‼	59	111011	;	99	1100011	c	139	10001011	ï	179	10110011	|	219	11011011	█			
20	10100	¶	60	111100	<100	1100100	d	140	10001100	î	180	10110100	┤	220	11011100	▄			
21	10101	§	61	111101	=	101	1100101	e	141	10001101	ì	181	10110101	╡	221	11011101	▌			
22	10110	▬	62	111110	>102	1100110	f	142	10001110	Ä	182	10110110	╢	222	11011110	▐			
23	10111	↨	63	111111	?	103	1100111	g	143	10001111	Å	183	10110111	╖	223	11011111	▀			
24	11000	↑	64	1000000	@	104	1101000	h	144	10010000	É	184	10111000	╕	224	11100000	α			
25	11001	↓	65	1000001	A	105	1101001	i	145	10010001	æ	185	10111001	╣	225	11100001	ß			
26	11010	→	66	1000010	B	106	1101010	j	146	10010010	Æ	186	10111010	║	226	11100010	Γ			
27	11011	←	67	1000011	C	107	1101011	k	147	10010011	ô	187	10111011	╗	227	11100011	π			
28	11100	∟	68	1000100	D	108	1101100	l	148	10010100	ö	188	10111100	╝	228	11100100	Σ			
29	11101	↔	69	1000101	E	109	1101101	m	149	10010101	ò	189	10111101	╜	229	11100101	σ			
30	11110	▲	70	1000110	F	110	1101110	n	150	10010110	û	190	10111110	╛	230	11100110	µ			
31	11111	▼	71	1000111	G	111	1101111	o	151	10010111	ù	191	10111111	┐	231	11100111	τ			
32	100000	(espacio)	72	1001000	H	112	1110000	p	152	10011000	ÿ	192	11000000	└	232	11101000	Φ			
33	100001	!	73	1001001	I	113	1110001	q	153	10011001	Ö	193	11000001	┴	233	11101001	Θ			
34	100010	"	74	1001010	J	114	1110010	r	154	10011010	Ü	194	11000010	┬	234	11101010	Ω			
35	100011	#	75	1001011	K	115	1110011	s	155	10011011	¢	195	11000011	├	235	11101011	δ			
36	100100	$	76	1001100	L	116	1110100	t	156	10011100	£	196	11000100	─	236	11101100	∞			
37	100101	%	77	1001101	M	117	1110101	u	157	10011101	¥	197	11000101	┼	237	11101101	φ			
38	100110	&	78	1001110	N	118	1110110	v	158	10011110	₧	198	11000110	╞	238	11101110	ε			
39	100111	(tilde)	79	1001111	O	119	1110111	w	159	10011111	ƒ	199	11000111	╟	239	11101111	∩			

El CCOS así definido satisface los criterios básicos para un contenedor óptimo. Primero, su contenido espectral puede deducirse fácilmente a partir de la separación y tamaño de los bloques. Por ejemplo, cuando todas las celdas corresponden a un 1 y el tamaño de bloque es igual a la separación, el contenedor es igual al producto de una red de Ronchi horizontal con otra vertical de la misma frecuencia. Segundo, la tolerancia al ruido del CCOS está directamente relacionado con la tolerancia al ruido, debido a que la intensidad promedio de cada celda no cambiara significativamente si el tamaño de bloque es grande comparado con el tamaño de speckle del sistema óptico. Por último, la lectura del CCOS es llevada a cabo con tres operaciones sencillas: una división del código en 9

celdas, el cálculo de las intensidades promedio de las celdas y por último la comparación con el valor límite para determinar si la celda corresponde a un 1 o a un 0.

Ahora procederemos a probar numéricamente el desempeño del código propuesto. Para ello, codificaremos una entrada, en este caso la letra "A", en un código QR y en un CCOS, y procederemos a someter los códigos resultantes a un proceso de encriptación-desencriptación con un criptosistema JTC simulado. Este proceso lo repetiremos hasta encontrar el tamaño mínimo en pixeles en el cual se puede codificar la letra de tal manera que el código desencriptado pueda ser leído satisfactoriamente.

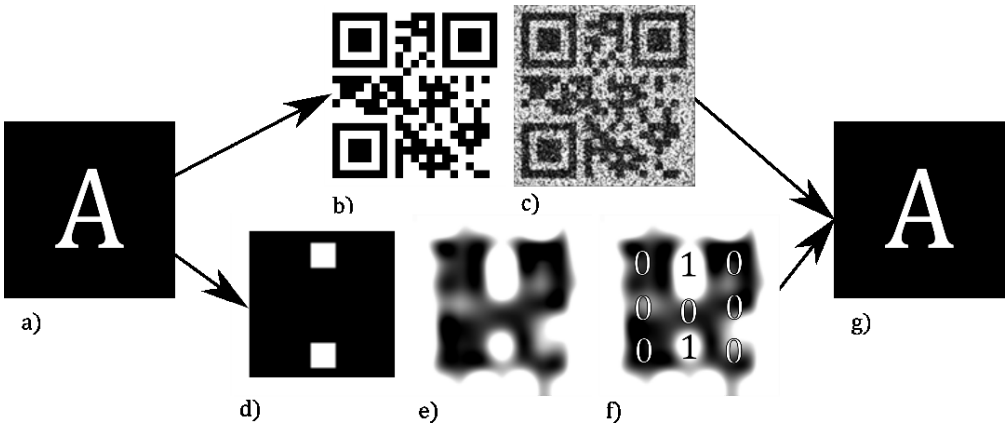

Figura 45: Tamaño mínimo para la encriptación-desencriptación con códigos QR y CCOS. a) carácter de entrada, b) código QR de a), c) código QR de a) tras el proceso de encriptación-desencriptación, d) CCOS de a), e) CCOS de a) tras el proceso de encriptación-desencriptación, f) valor de las celdas del CCOS desencriptado, y g) lectura de los códigos.

Los resultados de esta prueba se muestran en la *Figura 45.* El tamaño mínimo para que el código QR fuera legible fue de 150x150 pixeles (Figura 45.*c*), mientras que para el CCOS fue de tan solo 9x9 pixeles. Aunque el CCOS desencriptado presenta una fuerte degradación, la lectura (Figura 45.f) permite obtener el valor binario correspondiente a la letra original. El requerir de una menor cantidad de pixeles para su un procesado optimo nos hace inferir que el CCOS permite encriptar la misma información usando un sistema óptico más simple y compacto.

También se puede aprovechar esta ventaja de los CCOS para encriptar más información simultánea, simplemente codificando el mensaje en un arreglo de CCOS. Para mostrar esta capacidad, ahora codificaremos el mismo mensaje de 144 caracteres en un CCOS y un código QR con 200x200 pixeles de tamaño en ambos casos.

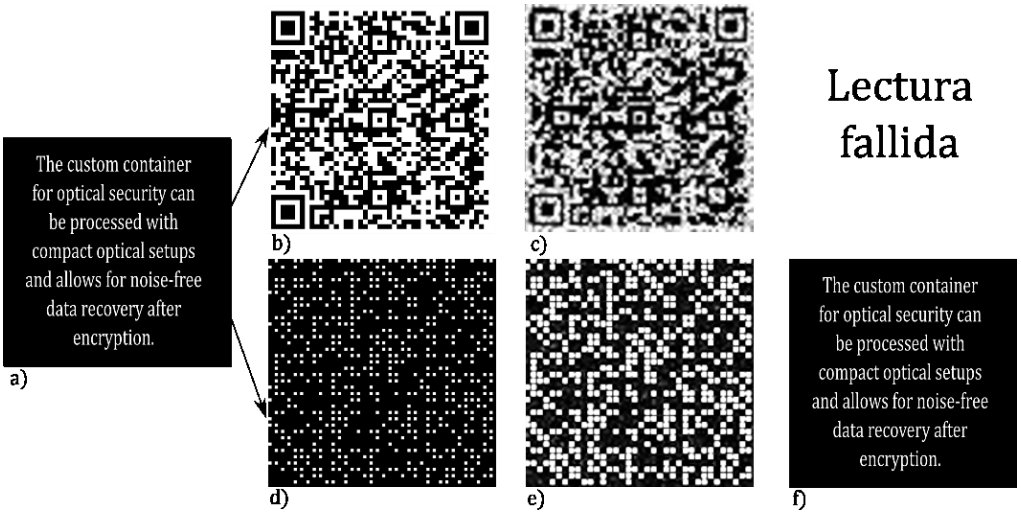

Figura 46: Resultado de encriptación-desencriptación de múltiples caracteres: a) mensaje de entrada, b) código QR de a), c) código QR tras encriptación-desencriptación, d) CCOS de a), e) CCOS tras encriptación-desencriptación, y f) lectura de e).

Como se puede apreciar en la Figura 46, con un área de 200x200 pixeles es posible encriptar satisfactoriamente el mensaje usando un código CCOS, sin embargo, cuando se intenta con un código QR, tras desencriptarlo la lectura falla. De esta manera, dado un sistema óptico capaz de procesar entradas de un área determinada, el CCOS permitirá encriptar más información que el código QR.

Ahora procederemos a comprobar la resistencia a la perdida de datos del código QR y del CCOS. Para ello, introducimos un creciente nivel de perdida de información aleatoriamente al texto cifrado correspondiente a los códigos de la Figura 45.b y d encriptados con un tamaño de 200x200 pixeles y calculamos el NMSE entre los resultados desencriptados con y sin perdida.

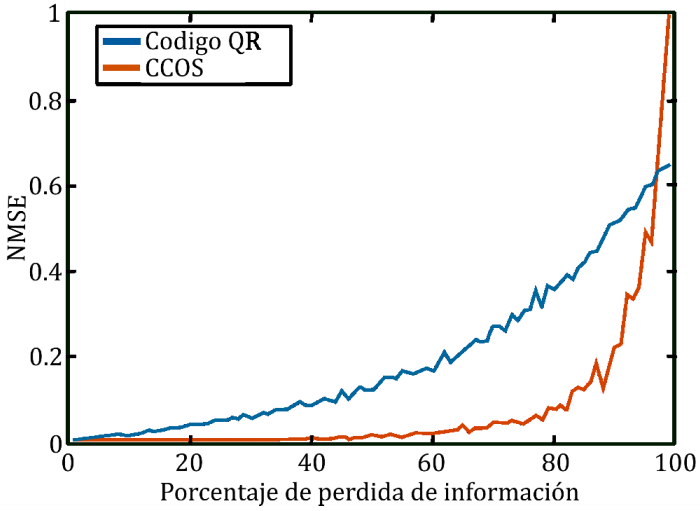

Figura 47: NMSE entre los códigos de la letra A desencriptados a partir de textos cifrados con y sin pérdida de información.

La Figura 47 muestra cómo los códigos QR sufren un aumento mayor del error conforme se pierde información, mientras que no sucede lo mismo con los CCOS. En el caso de estos últimos, el error se mantiene más bajo que en los códigos QR hasta que la perdida es mayor al 96%. También probamos la legibilidad de los códigos afectados por la perdida. El código QR deja de ser legible cuando la perdida es igual o mayor que 60%, mientras que el CCOS se mantiene legible con perdida de hasta el 92%, como se muestra en la Figura 48.

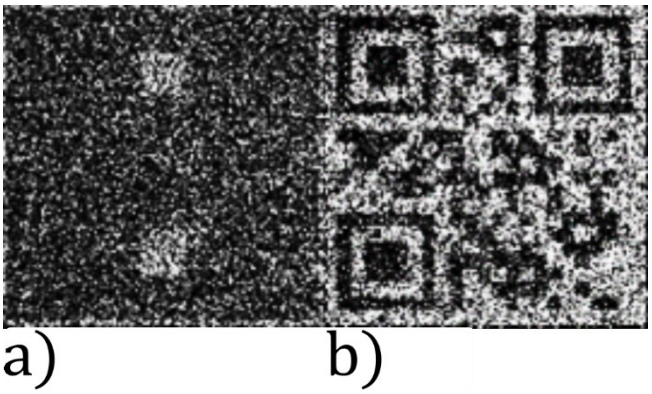

Figura 48: Códigos desencriptados con el máximo nivel de perdida permitido para su lectura. A) CCOS con 92% de perdida y b) código QR con 60% de perdida.

Los resultados numéricos obtenidos anteriormente demuestran la efectividad de los CCOS sobre los códigos QR para su uso en aplicaciones basadas en DRPE. Para respaldar esta conclusión, verificaremos el desempeño de nuestra propuesta en un sistema óptico real. Para ello, usamos el montaje descrito en la Figura 25, con una cámara CMOS EO-10012C de 3840x2748 de resolución y tamaño de pixel de $1.67\,\mu m \times 1.67\,\mu m$ como medio de registro y un láser DPSS de 532 nm de longitud de onda con $300\,mW$ de potencia. El objeto y la ventana de la llave fueron proyectados usando un modulador espacial de luz HOLOEYE LC2000, con tamaño de pixel de $32\,\mu m \times 32\,\mu m$. Se uso una lente de 200 mm de distancia focal.

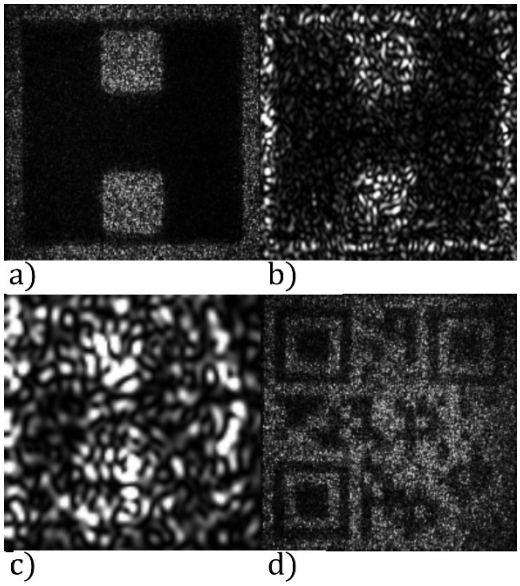

Figura 49: Resultados experimentales de encriptación-desencriptación de contenedores de la letra "A": a) CCOS de 6.4 mm x 6.4 mm, b) CCOS de 1.6 mm x 1.6 mm, c) CCOS de 0.64 mm x 0.64 mm y d) Código QR de 6.4 mm x 6.4 mm.

Para la prueba experimental, sometimos CCOS y códigos QR de la misma letra, con distintos tamaños, al proceso de encriptación-desencriptación, verificando si el resultado era legible. El tamaño máximo que permite nuestro sistema fue de 6.4 mm x 6.4 mm, equivalente a un código de 200x200 pixeles. Los resultados muestran que el CCOS con un tamaño de 0.64 mm x 0.64 mm continúa siendo legible, a pesar de presentar un alto grado de degradación (Figura 49.c). El código QR, sin embargo, no es legible ni usando el tamaño máximo de 6.4 mm x 6.4 mm (Figura 49.d).

Con vistas a los resultados obtenidos, es claro que el CCOS permite un gran aumento en la tolerancia al ruido respecto al código QR, a la vez que su encriptación satisfactoria requiere de menos espacio en el plano de entrada, aumentando la cantidad de información que puede ser procesada simultáneamente en un criptosistema óptico. El CCOS fue diseñado con criterios relativamente simples, por lo que no necesariamente es el contenedor de información ideal, sin embargo demuestra que el concepto de diseñar los contenedores específicamente para las características del sistema óptico en el que van a ser utilizado, puede ayudar a superar algunas de las limitaciones causadas por el ruido

.

2.8. Reducción de ruido.

El ruido de speckle es un problema inherente a los sistemas con iluminación coherente [59], y limita las posibles aplicaciones de estos. Los contendores de información como el CCOS son una forma de reducir los efectos del ruido. Sin embargo, la codificación y lectura de los contenedores añade complejidad al sistema de encriptación, lo cual puede ser un inconveniente para aplicaciones que requieran alta velocidad de procesamiento.

Adicionalmente, conforme mayor sea el volumen de información que se quiere introducir en un código, mayor será su complejidad. En el caso de textos, cada carácter puede ser representado en 8 bits, haciendo simple su codificación en un contenedor, pero en una imagen en escala de grises, cada pixel requiere 8 bits para almacenar su nivel de intensidad. Esto implica que para codificar una imagen de 50x50 pixeles en un CCOS serían necesarios 2500 CCOS, que suponiendo un tamaño mínimo de lectura de 9x9 pixeles, ocuparían 450x450 pixeles, un aumento significativo en el área necesaria en el plano de entrada para garantizar encriptación exitosa.

Es por este motivo que, a pesar de propuestas como los CCOS, reducir el ruido presente en la desencriptación continúa siendo de gran interés, si se desea procesar objetos más complejos y o que involucren mayores volúmenes de información.

La dificultad en la reducción de ruido en el DRPE radica en que existen múltiples arquitecturas como el JTC y el 4f, y las causas de la degradación de los datos encriptados pueden variar entre cada una de ellas. Adicionalmente, los estudios sobre reducción de ruido en sistemas simulados no necesariamente son de utilidad para encontrar soluciones a este problema en los sistemas ópticos reales. Esto se debe a que en los sistemas ópticos reales aparecen factores como las vibraciones, perturbaciones atmosféricas, y los defectos propios de los elementos ópticos que son difíciles de tener en cuenta en los experimentos numéricos.

En nuestro caso, para tratar de entender el problema del ruido, partiremos del supuesto de que el DRPE es un sistema holográfico cuya onda de referencia es una función aleatoria, tal y como se expuso en la sección 2.2. Siguiendo este razonamiento, podemos esperar que los objetos recuperados a partir de datos encriptados ópticamente con un

criptosistema JTC estén sujetos a las mismas fuentes de ruido que los reconstruidos a partir de un holograma de Fourier.

Si verificamos esta suposición con una simulación numérica, en la cual usamos el mismo objeto de entrada para ambos casos, nos encontramos que el objeto reconstruido a partir de un holograma no sufre de deterioro alguno (Figura 50.a), cosa que si ocurre con el objeto desencriptado (Figura 50.b).

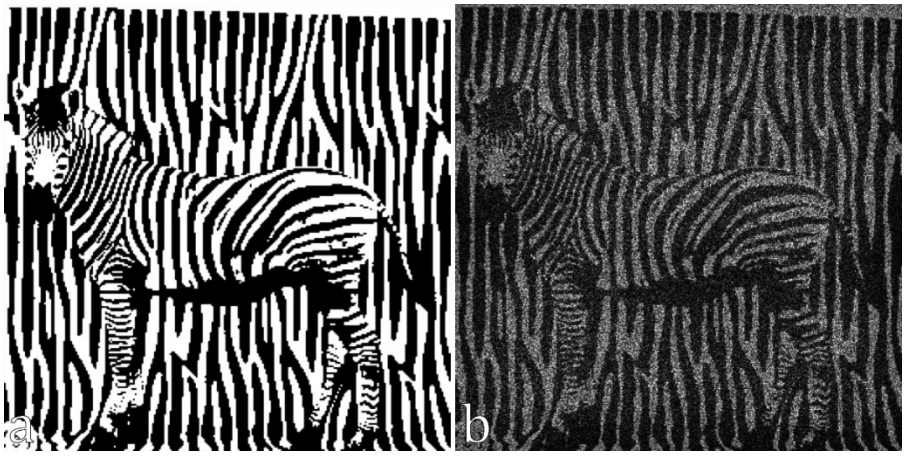

Figura 50: Objetos recuperados numéricamente a partir de: a) un holograma de Fourier, b) el mismo dato encriptado con un sistema JTC.

Este resultado nos indica que la degradación que presentan los datos procesados con DRPE es introducida por el uso de funciones aleatorias como onda de referencia. Recordando la expresión de un objeto desencriptado, tenemos que es de la forma

$$d(x,y) = c(x,y) \otimes k^*(x,y) \otimes k(x,y) \qquad (2.8.1)$$

donde $c(x,y) = o(x,y)r(x,y)$, $o(x,y)$ es el objeto, y $r(x,y)$, $k(x,y)$ son funciones de fase aleatorias. De la expresión anterior podemos concluir que sí $k(x,y) \otimes k^*(x,y) = \delta(x,y)$, la reconstrucción será perfecta. En la práctica, solo hay dos formas de que esta condición se cumpla: primero, que la TF de $k(x,y)$ sea de una función de fase pura o segundo, que la llave sea infinita en extensión.

Estas condiciones son extremadamente difíciles de satisfacer, la segunda por motivos obvios, y la primera por que los elementos usados para reproducir funciones de fase pura en el laboratorio, como los moduladores espaciales de luz o los difusores, no son ideales.

Aunque se conocía que la realización practica de los DRPE no reproducía las condiciones exactas de su formulación teórica, la mayoría de los trabajos para disminuir

el ruido se centraron en buscar arquitecturas donde la condición de reconstrucción se cumpliera. Vilardi *et al* [48], por otro lado, propusieron una modificación para reducir el ruido sin alterar la arquitectura del criptosistema.

La modificación consiste en dividir el objeto encriptado por la intensidad de la transformada de Fourier de la llave, tal que

$$E(v,w) = \frac{C(v,w)K^*(v,w)}{|K(v,w)|^2} \tag{2.8.2}$$

Al multiplicar este nuevo objeto encriptado por la llave obtenemos

$$\begin{aligned} D(v,w) &= \frac{C(v,w)K^*(v,w)K(v,w)}{|K(v,w)|^2} \\ &= \frac{C(v,w)|K(v,w)|^2}{|K(v,w)|^2} = C(v,w) \end{aligned} \tag{2.8.3}$$

de la ecuación anterior, podemos ver que tras una TFI se recupera el objeto original sin ningún termino adicional que pueda causar degradación. Esta modificación no lineal, a pesar de que aparentemente puede eliminar todos los efectos del ruido sobre la reconstrucción, tiene algunas desventajas importantes. Primero, requiere que se capture la información de la intensidad de la TF de la llave, lo que añade un paso extra en el proceso de encriptación. Segundo, la operación de división no se puede llevar a cabo ópticamente, añadiendo más procesado digital a los datos registrados. Ademas, esta operación no puede llevarse a cabo directamente, pues en los puntos en los que los valores de $|K(v,w)|^2$ sean iguales a cero se producirán indeterminaciones.

Esto obliga a que antes de realizar la división, se reemplacen los valores cercanos a cero de $|K(v,w)|^2$ por valores más grandes. El realizar este proceso hace que no sean iguales las intensidades de la TF de la llave que se encuentran en el denominador y el numerador, por lo que el ruido no se elimina totalmente. Además, la elección del límite por debajo del cual se debe reemplazar el valor de $|K(v,w)|^2$ tiene un fuerte efecto en el grado de reducción de ruido que se puede alcanzar, y varía dependiendo de la llave usada.

Otra modificación que permite reducir el ruido fue propuesta por Barrera *et al* [60], y consiste en desencriptar usando sólo la fase de la TF de la llave. Así, tenemos que la TF de la llave es dada por

$$K(v,w) = |K(v,w)|\, e^{i\phi(v,w)} \tag{2.8.4}$$

donde $\phi(v,w)$ es la fase de $K(v,w)$. Al multiplicar el dato encriptado por esta fase, obtenemos

$$\begin{aligned} D(v,w) &= C(v,w)K^{*}(v,w)e^{i\phi(v,w)} \\ &= C(v,w)\,|K(v,w)|\,e^{-i\phi(v,w)}e^{i\phi(v,w)} \\ &= C(v,w)\,|K(v,w)| \end{aligned} \tag{2.8.5}$$

Al realizar la TFI de la ecuación anterior se obtiene

$$d(x,y) = c(x,y) \otimes TFI\left[|K(v,w)|\right] \tag{2.8.6}$$

La expresión anterior corresponde al objeto, convolucionado con la TFI de la amplitud de $K(v,w)$, lo que introduce degradación. Sin embargo, si $K(v,w)$ tiene poca variación en su amplitud, su transformada de Fourier inversa se aproximará más a una delta de Dirac que su autocorrelación, disminuyendo así el ruido con respecto a la desencriptación convencional.

Esta última técnica no causa una reducción en el ruido tan significativa como la que se puede lograr con la modificación no lineal, pero se puede llevar a cabo sin necesidad de registrar ningún dato adicional, y no requiere de divisiones que puedan dar lugar a indeterminaciones.

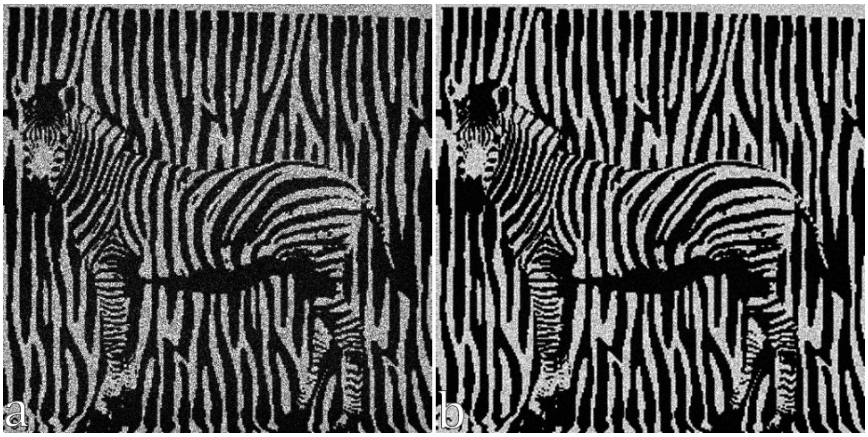

Figura 51: Resultados de la desencriptación con reducción de ruido: a) desencriptación con solo fase, b) desencriptación con modificación no lineal.

En la Figura 51 se muestra el efecto de aplicar los métodos de reducción de ruido expuestos con anterioridad al objeto encriptado con el que se obtuvo el resultado de la Figura 50b. Aunque en ambos casos se logra una reducción significativa del ruido, la

modificación no lineal (Figura 51b) presenta un desempeño ligeramente superior a la desencriptación con solo la fase (Figura 51a).

Debido a los inconvenientes que mencionamos anteriormente, la modificación no lineal produce una reducción mucho más modesta cuando se aplica a resultados obtenidos en sistemas ópticos reales. Para mostrar esto, encriptamos el mismo texto plano de la Figura 50 usando el criptosistema experimental de la sección 2.3.

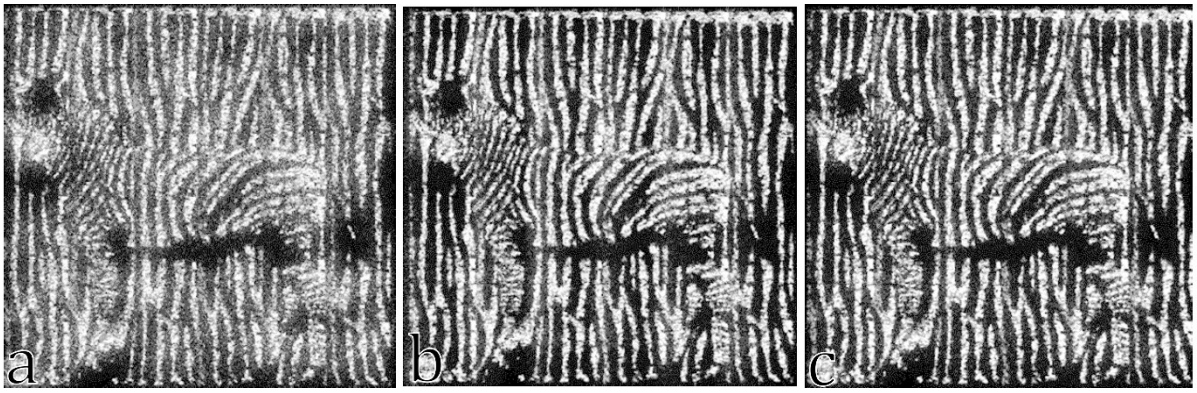

Figura 52: Objeto desencriptado con un sistema JTC experimental usando: a) desencriptación convencional, b) desencriptación con solo fase, y c) desencriptación con modificación no lineal.

En efecto, en los resultados de la Figura 52 podemos constatar que en un sistema experimental, la modificación no lineal resulta en una mejora de calidad muy similar a la obtenida con la desencriptación solo con fase, por lo cual esta última es de mayor utilidad en la mayoría de las aplicaciones experimentales debido a su simplicidad.

A continuación presentamos otra estrategia de reducción de ruido, la cual fue demostrada por Velez *et al* [61]. En este trabajo proponemos un método en el cual se altera la forma en la que se proyectan los objetos de entrada del criptosistema. Para explicar el razonamiento detrás de esta modificación primero analizamos la autocorrelación de la llave $k(x,y)\otimes k^{*}(x,y)$.

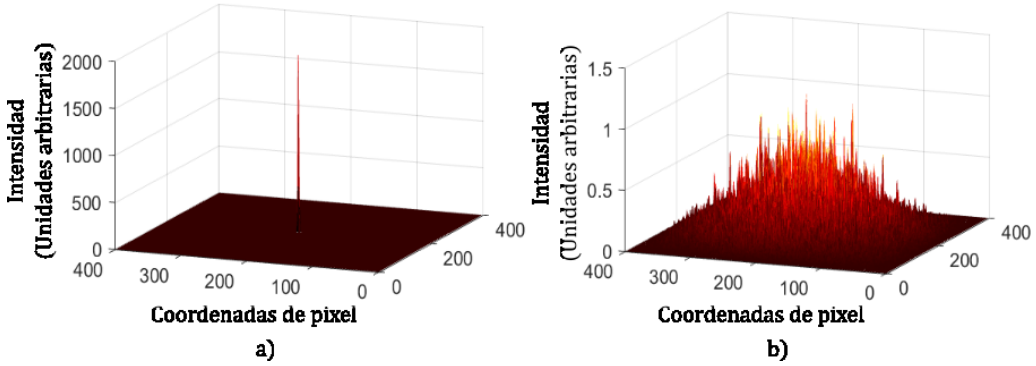

Figura 53: a) autocorrelación de una función de fase aleatoria de 200x200 pixeles, b) autocorrelación de la misma función con el pico central suprimido.

Esta autocorrelación tiene la forma de una delta de Dirac (Figura 53a), rodeada de un ruido de baja intensidad, como se puede observar en la Figura 53b tras suprimir el pico central. Este ruido de correlación aleatoria, (RCN por las siglas en inglés de "random correlation noise") es el responsable de la degradación que afecta los datos desencriptados, a pesar de su muy baja intensidad. Si consideramos un texto plano como un arreglo de puntos discretos, tras la desencriptación obtendremos cada punto de éste convolucionado con el RCN. Así, el ruido de puntos cercanos se superpone, causando un rápido aumento en la intensidad del mismo.

Teniendo en cuenta esta característica del RCN, es posible reducir su efecto de forma significativa separando digitalmente un texto plano en puntos (pixeles) con un espaciado entre ellos. Esto reduce la superposición del ruido, limitando así su intensidad. Esta técnica de separación de pixeles (PST por las siglas en inglés de "pixel separation technique") puede además combinarse con métodos como el de desencriptación de solo fase o no lineal, para lograr una reducción aún mayor en la degradación de los objetos desencriptados.

Para demostrar la efectividad de nuestra propuesta, encriptamos el mismo texto plano numéricamente, sin ninguna modificación, y luego introduciendo separaciones de 1 y 2 pixeles entre cada pixel del texto plano original, para posteriormente desencriptar los datos cifrados con el método convencional.

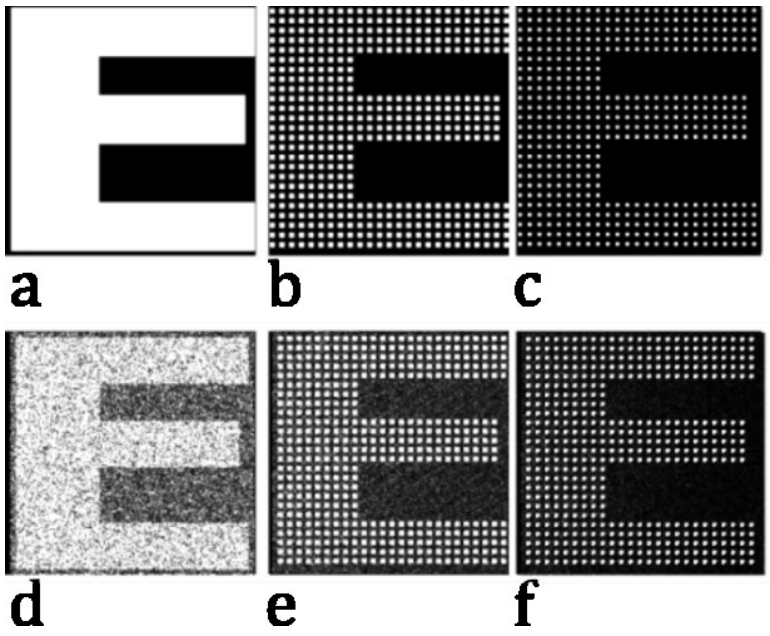

Figura 54: Resultados de desencriptación numérica: a), b) y c) texto plano original y con 1 y 2 pixeles de separación, respectivamente, d), e) y f) objetos desencriptados correspondientes a a), b) y c).

Como se muestra en la Figura 54.d, el objeto recuperado sin separación entre pixeles presenta un elevado nivel de ruido tras la desencriptación, el cual se ve disminuido cuando se introduce un pixel de separación (Figura 54.e) y es casi imperceptible cuando se introducen 2 (Figura 54.f). De esta manera, podemos garantizar que un objeto cualquiera sufra de menos degradación debido al RCN introduciendo una separación entre sus pixeles. Tras desencriptar el objeto, se revierte digitalmente la separación de pixeles, recuperando el texto plano original.

Para cuantificar el efecto del PST, ahora procederemos a encriptar el mismo texto plano con creciente separación entre sus pixeles, calculando el NMSE entre el texto plano original y los textos planos desencriptados tras deshacer la separación. El resultado se puede apreciar en la Figura 55, donde constatamos que el error disminuye rápidamente con una pequeña separación. A partir de 4 pixeles de separación, aunque el error no es cero, la imagen desencriptada es prácticamente indistinguible de la original, y mayores separaciones contribuyen poco a la reducción de ruido.

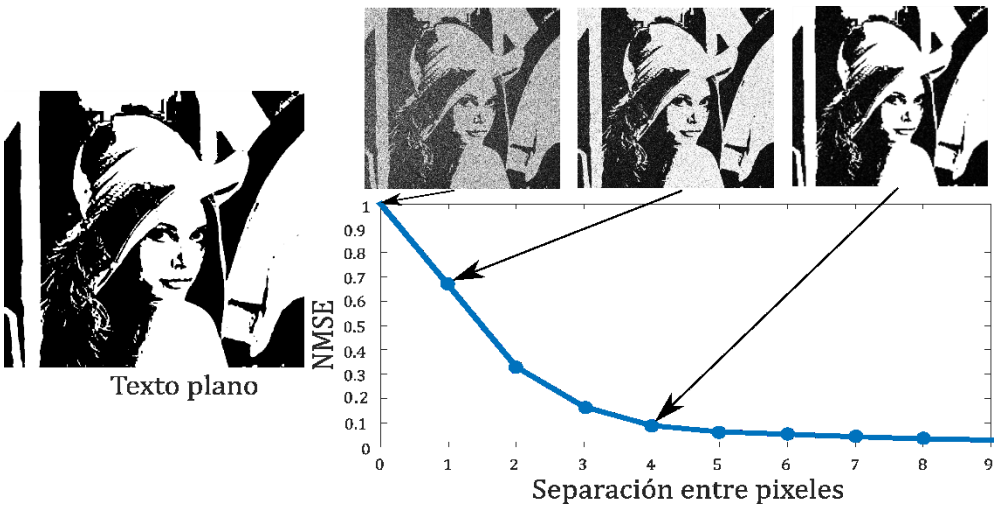

Figura 55: NMSE entre el texto plano original y los objetos desencriptados a partir del mismo texto plano sometido a PST.

A continuación, procederemos a verificar experimentalmente el desempeño del PST. Para ello, usaremos de nuevo el esquema experimental de la sección 2.3 para encriptar tres textos planos distintos. Los objetos tuvieron dimensiones máximas de 12.8 mm x

12.8 mm, que equivale a 400x400 pixeles proyectados en un modulador Holoeye LC 2002 de 800x600 de resolución y 32 $\mu m \times 32\ \mu m$ de tamaño de pixel.

En la Figura 56.a se muestran los textos planos proyectados en el modulador, y en la Figura 56.b el resultado tras el proceso de encriptación-desencriptación. En la Figura 56.c se muestra el texto plano proyectado con separación de 2 pixeles, y en la Figura 56.d los objetos desencriptados. En la Figura 56.e se muestra el objeto obtenido tras deshacer digitalmente la separación. Hemos así mostrado que la aplicación del PST da lugar a una reducción significativa del ruido. Teniendo en cuenta el caso del código QR, si no se aplica la técnica propuesta no es posible obtener un resultado legible.

Vale la pena señalar que hasta ahora nos hemos centrado en objetos binarios. Esto es debido a que en el procesamiento de datos en escala de grises cobran importancia otras fuentes de ruido a parte del RCN, las cuales discutiremos a continuacion.

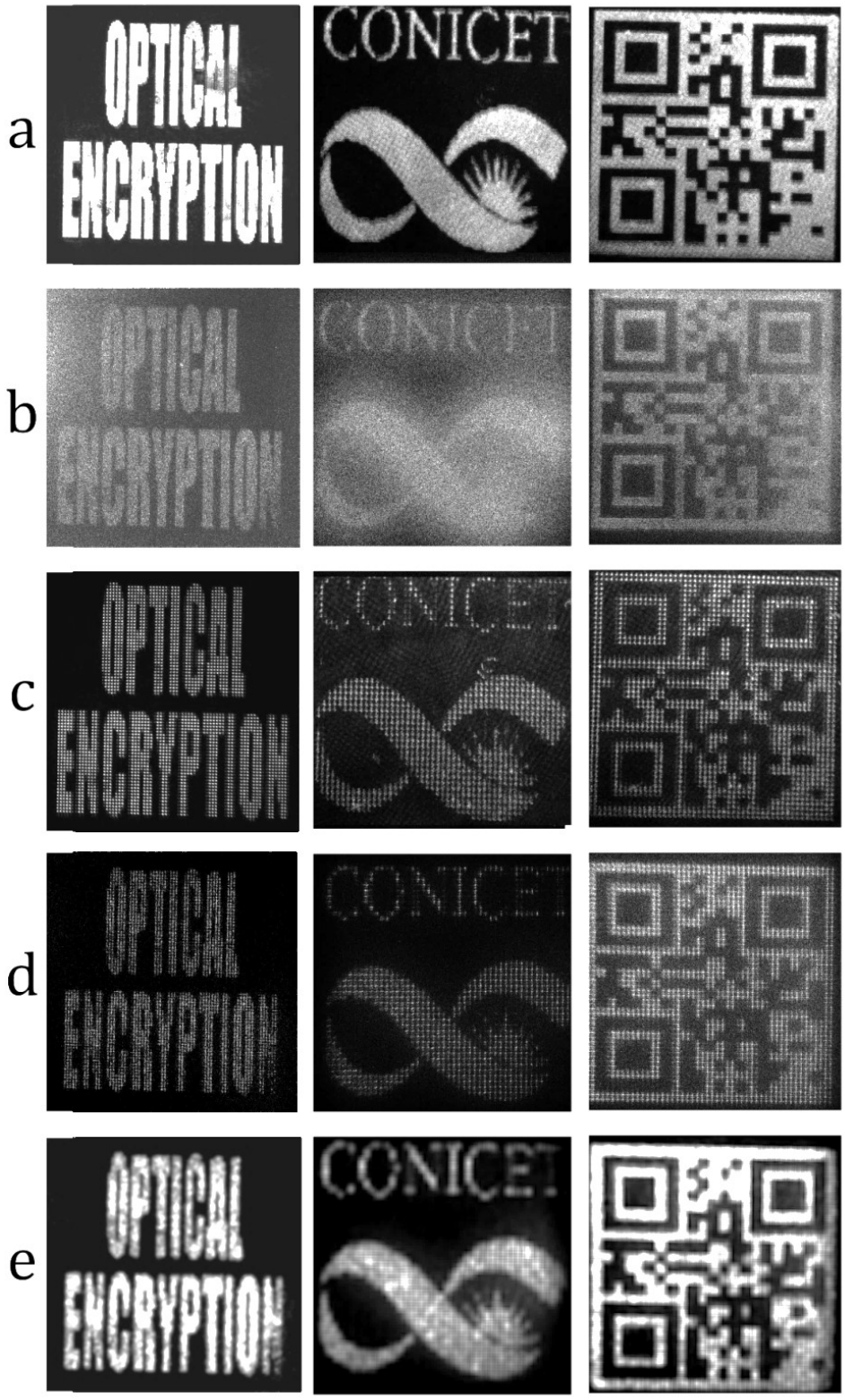

Figura 56: Resultados experimentales de reduccion de ruido con PST: a) objetos de entrada, b) desencriptacion convencional, c) objetos de entrada con PST de 2 pixeles, d) desencriptacion de c),

En Velez *et al* [62] mostramos que es posible combinar las distintas técnicas ya presentadas, y algunas nuevas, con el propósito de reducir el ruido en la encriptación

experimental de objetos en escala de grises, analizando paso a paso las distintas fuentes de ruido que causan deterioro de los objetos encriptados.

La primera dificultad a la que nos enfrentamos para la reducción de ruido experimental tiene que ver con una característica de los medios de registro digitales. En la sección 1.4 se discutieron las condiciones necesarias para la captura de hologramas digitales, sin embargo, estas condiciones suponen que el muestreo debido a una cámara digital es ideal, es decir, que el sensor es un arreglo de deltas de Dirac que muestrean el campo, con una separación entre ellas igual al tamaño de pixel.

En realidad, cada pixel registra los puntos del campo en el espacio que este ocupa. Esto implica que una imagen tomada por una cámara digital es de la forma

$$R(x,y)=\sum_{n,m}^{N,M} rect\left(\frac{x-x_n}{\Delta x},\frac{y-y_m}{\Delta y}\right)\otimes\left|o(x,y)\right|^2 \qquad (2.8.7)$$

Donde $o(x,y)$ es el campo que llega a la cámara, (x_n,y_m) son las coordenadas del pixel (n,m), N, M es el número de pixeles en cada dirección, y Δx , Δy es el tamaño de pixel. Reescribiendo lo anterior obtenemos

$$R(x,y)=\sum_{n,m}^{N,M}\delta(x-x_m,y-y_m)\otimes rect\left(\frac{x}{\Delta x},\frac{y}{\Delta y}\right)\otimes\left|o(x,y)\right|^2 \qquad (2.8.8)$$

Cuando se realiza la TFI de la ecuación anterior obtenemos

$$r(v,w)=\sum_{n,m}^{N,M} e^{-2\pi i(x_n v+y_m w)}\left|\Delta x\Delta y\right|\mathrm{sinc}\left(v\Delta x,w\Delta y\right)TFI(|\,o(x,y)\,|^2) \qquad (2.8.9)$$

El producto con la función sinc en la ecuación anterior hace que las frecuencias altas sufran una disminución en la amplitud respecto a las bajas. En la reconstrucción de datos encriptados, y en los hologramas de objetos extensos, esto causa que las partes del objeto recuperado cercanas al centro del plano de reconstrucción tengan mayor intensidad que las que están más lejos. Para evitar este problema se puede dividir la TFI del registro por una función sinc igual a la de la ecuación (2.8.9). También se puede usar una ventana de Hamming, la cual es un coseno con su máximo en el centro del plano y sus mínimos en los extremos, más un valor constante para evitar que la función sea cero en los mismos [63]. Usando la ventana de Hamming se obtiene una corrección adecuada de la intensidad para la mayoría de las cámaras digitales.

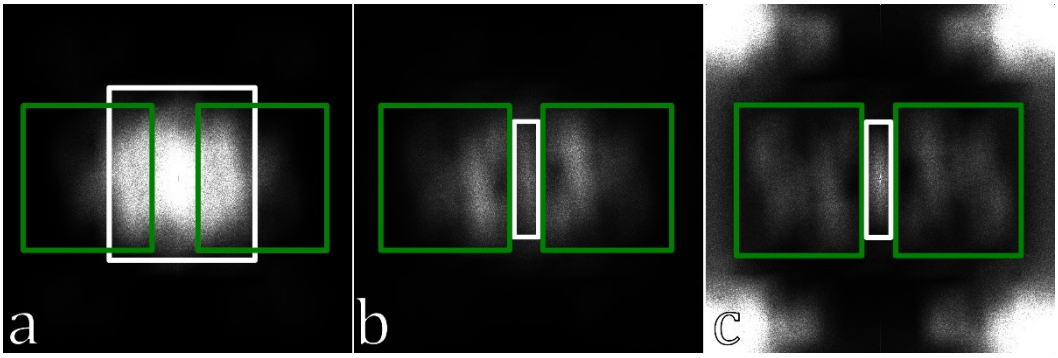

Figura 57: a) intensidad de la TF de un JPS, b) intensidad de a) tras sustraer la intensidad de la FT de la llave y el objeto, y c) intensidad de b) tras dividir por la ventana de Hamming.

En la Figura 57 se muestra el efecto de la corrección de intensidad durante el filtrado de un JPS registrado experimentalmente con el esquema de la sección 2.3. Los cuadros verdes corresponden a la TF del objeto encriptado y su complejo conjugado, y el blanco al orden central. En la Figura 57.a se aprecia como el orden central se superpone con el objeto encriptado, y no es posible filtrarlo satisfactoriamente. Tras sustraer la intensidad de la TF de la llave y el objeto, como se describió en la sección 1.5, el orden central se reduce significativamente, permitiendo un filtrado adecuado (Figura 57.b), sin embargo, la intensidad del orden correspondiente al objeto encriptado es mayor cerca al centro del plano. Al dividir por la ventana de Hamming, la intensidad de éste se ecualiza en toda su extensión, como se puede apreciar en la Figura 57.c.

Ahora bien, si suponemos que la aplicación del PST y la modificación no lineal eliminan completamente el efecto del RCN, tenemos un dato desencriptado dado por

$$d(x,y)=[o(x,y)r(x,y)] \qquad (2.8.10)$$

donde $o(x,y)$ es el objeto y $r(x,y)$ es una máscara aleatoria de fase. Así, sacando la intensidad de la ecuación anterior, se puede eliminar la máscara de fase y se obtiene la intensidad del dato encriptado. En la práctica, la máscara de fase $r(x,y)$ es generada por un difusor, por lo que no es una función de fase pura, sino que es una función aleatoria tanto en fase como en amplitud, introduciendo así una degradación en el objeto reconstruido.

Para eliminar este efecto, proponemos encriptar una función rect multiplicada por la máscara de fase $r(x,y)$, para así obtener la información de su amplitud, sometida a las mismas fuentes de ruido que $o(x,y)$. Si aplicamos las mismas técnicas de reducción de

ruido a esta “mascara de referencia” y luego la desencriptamos, se puede dividir el objeto recuperado en la ecuación (2.8.10), por el resultado obtenido, tal que

$$d_r(x,y) = \frac{o(x,y)r(x,y)}{r(x,y)} \tag{2.8.11}$$

De la expresión anterior, podemos suponer que se eliminan los efectos debido a la variación en amplitud de la máscara de fase $r(x,y)$. Por supuesto, este método tiene las mismas limitaciones que la modificación no lineal, es decir, se debe alterar $r(x,y)$ al dividir para evitar indeterminaciones, y requiere el registro de datos adicionales, por lo que en la práctica no se eliminará el ruido totalmente. Además, la división por la máscara de referencia requiere que previamente se logre suprimir el ruido debido al RCN en un alto grado, pues de lo contrario se obtiene

$$d_r(x,y) = \frac{o(x,y)r(x,y) \otimes k^*(x,y) \otimes k(x,y)}{r(x,y) \otimes k^*(x,y) \otimes k(x,y)} \tag{2.8.12}$$

lo que implica que, en lugar de reducir el ruido, éste se verá aumentado. A pesar de la complejidad que se le añade al DRPE con estas modificaciones, como mostraremos a continuación, se puede lograr la recuperación de objetos complejos en escala de grises que de lo contrario se verían seriamente deteriorados. Adicionalmente, ninguno de estos métodos requiere alterar el esquema óptico. Así pues, proponemos un protocolo de reducción de ruido con los siguientes pasos

1. Aplicar el PST al objeto de entrada para reducir el RCN.

2. Sustraer la intensidad de la TF del objeto y la llave a la TF del JPS.

3. Dividir la TF del JPS por una ventana de Hamming para ecualizar la amplitud del objeto encriptado en todo el plano.

4. Filtrar el objeto encriptado

5. Aplicar la modificación no lineal.

6. Registrar la máscara de referencia aplicando los pasos 1-5, y luego dividir el objeto desencriptado por la máscara de referencia desencriptada.

Para mostrar la efectividad de nuestra propuesta se usó el esquema de la sección 2.3 con una cámara CMOS EO-10012C de 3840x2748 de resolución y tamaño de pixel de 1.67

$\mu m \times 1.67\ \mu m$ como medio de registro y un láser DPSS de 532 nm de longitud de onda con 300 mW de potencia. El objeto y la ventana de la llave fueron proyectados usando un modulador espacial de luz HOLOEYE LC2000, con tamaño de pixel de $32\ \mu m \times 32\ \mu m$. Se usó una lente de 200 mm de distancia focal. Los objetos proyectados sin PST tienen resolución de 600x600 pixeles, y los proyectados con PST resolución de 200x200 pixeles, divididos en bloques de 2 pixeles con una separación entre sí de 4 pixeles.

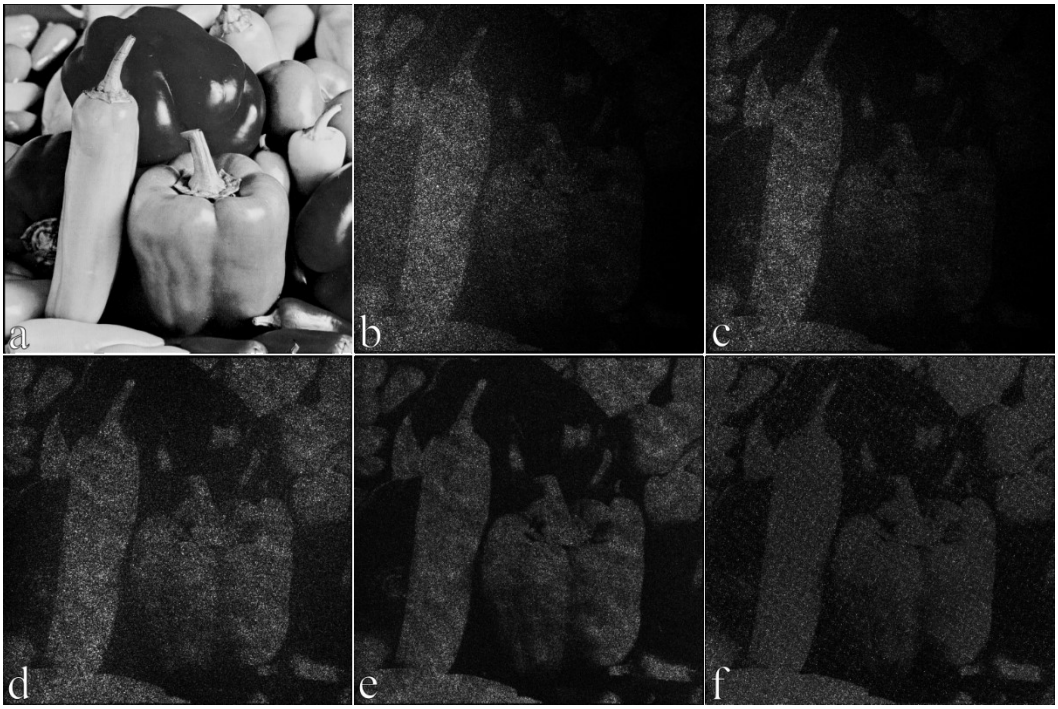

Figura 58: Procesado de la imagen a) usando: b) desencriptación convencional, c) desencriptación convencional con supresión del orden central durante el filtrado, d) desencriptación convencional con supresión del orden central y división con ventana de Hamming, e) desencriptación de d) con modificación no lineal y f) desencriptación de e) tras dividir por la máscara de referencia.

En la Figura 58 se muestra el efecto de los distintos pasos del protocolo de reducción de ruido sin aplicación del PST. Al desencriptar directamente (Figura 58.b), recuperamos el objeto con una intensidad no uniforme, y gran cantidad de ruido debido a la superposición con el orden central. Este ruido disminuye al sustraer las TF de la ventana de la llave y el objeto, pero el resultado continúa presentando una intensidad no uniforme (Figura 58.c). Si se divide por la ventana de Hamming durante el filtrado, se ecualiza la intensidad, aumentando significativamente la calidad del objeto desencriptado, sin embargo, todavía hay degradación debido al RCN (Figura 58.d). Aplicando la modificación no lineal se aumenta aún más la calidad de la reconstrucción (Figura 58.e). En la Figura 58.f, se muestra el resultado tras dividir por la máscara de referencia. Este objeto

presenta más ruido que el anterior, debido a que la modificación no lineal por sí sola no reduce suficientemente el RCN.

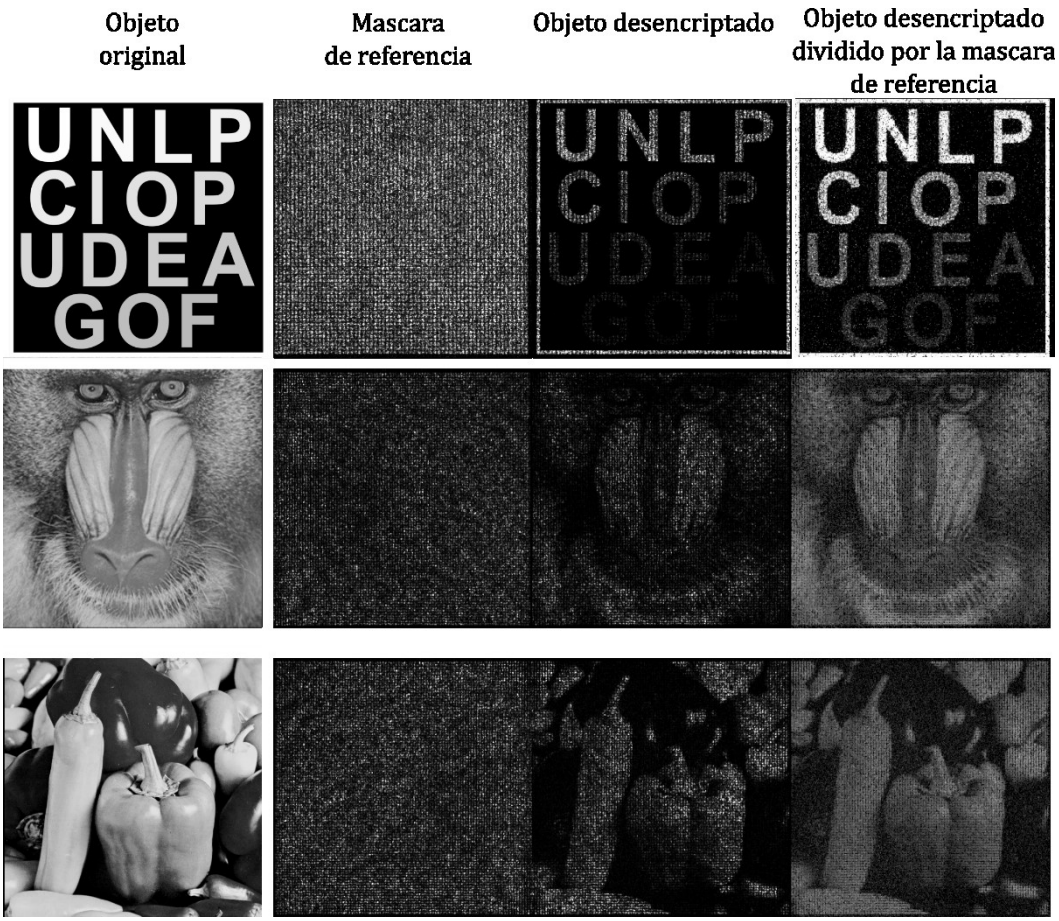

Figura 59: Resultados de desencriptación de tres objetos con el protocolo completo de reducción de ruido.

En la Figura 59 se muestran los resultados de aplicar el protocolo completo de reducción de ruido, incluido el PST. A diferencia del resultado de la Figura 58.f, al dividir por la máscara de referencia los objetos encriptados con PST, se obtiene un gran aumento de la calidad en el resultado final. Por supuesto, todavía hay ruido, sin embargo, ahora es posible distinguir los diferentes niveles de intensidad de las imágenes reconstruidas y detalles pequeños que antes no eran reconocibles.

Adicionalmente, hay un aumento en el contraste de los objetos recuperados respecto a los originales. Este efecto es causado por que el modulador espacial de luz usado para proyectar los objetos no tiene una respuesta lineal en amplitud.

Para cuantificar el efecto del protocolo propuesto, se calculó el coeficiente de correlación entre el objeto original y los resultados obtenidos aplicando cada operación de reducción de ruido. El coeficiente de correlación está definido como

$$r = \frac{\sum_{m,n}^{N,M} (A_{mn} - \bar{A})(B_{mn} - \bar{B})}{\sqrt{\left(\sum_{m,n}^{N,M} (A_{mn} - \bar{A})^2 \right) \left(\sum_{m,n}^{N,M} (B_{mn} - \bar{B})^2 \right)}} \qquad (2.8.13)$$

Donde m,n son coordenadas de pixel, A y B son las imágenes a correlacionar y $\bar{A}, \bar{B}$ son sus valores medios.

Tabla 2: Coeficientes de correlación de objetos desencriptados.

Proceso	Coeficiente de correlación (Letras)	Coeficiente de correlación (Mandril)	Coeficiente de correlación (Pimentones)
Desencriptación directa	0.1977	0.3612	0.4155
Supresión del orden central	0.4049	0.4469	0.5030
División con ventana de Hamming	0.4731	0.5841	0.6400
Modificación no lineal	0.5201	0.6240	0.7295
PST	0.6915	0.6688	0.7490
División con máscara de referencia	0.7531	0.7869	0.8088

Como se puede observar en la Tabla 2, usando el protocolo completo logramos duplicar el coeficiente de correlación respecto al obtenido con la desencriptación directa. Aunque el registro de la TF de la llave y la máscara de referencia añade complejidad al DRPE, vale la pena señalar que esto sólo debe llevarse a cabo si se desea cambiar la llave, de lo contrario se pueden procesarse todos los objetos deseados sin necesidad de repetir estos pasos. En el trabajo original donde se propuso este protocolo, se respaldó esta afirmación mostrando videos encriptados.

Así con el protocolo propuesto es posible encriptar gran cantidad de datos experimentalmente con niveles de calidad muy por encima de los obtenidos hasta ahora. Vale la pena señalar, que la aplicación de este protocolo en un sistema virtual es capaz de lograr una reducción del 100% del ruido.

2.9. Encriptación de objetos 3D.

Como última sección en este capítulo, se mostrará que los sistemas DRPE pueden ser usados para procesar datos 3D usando como llaves otros objetos 3D. Esta posibilidad es consistente con el hecho de que en la formulación de los DRPE que dedujimos en la sección 2.2 no impusimos ninguna restricción particular al objeto. Enrique Tajahuerce & Bahram Javidi demostraron la encriptación de objetos 3D [64].

Sin embargo, ya que las especificaciones de los DRPE requerían el uso de máscaras de sólo fase, en esta propuesta y otras para la encriptación de objetos 3D, se usaron llaves generadas por medio de difusores. En Velez *et al* [65] proponemos usar como llave otro objeto difuso 3D, en lugar de un difusor 2D, para lograr encriptar datos 3D usando una arquitectura JTC.

Por supuesto, usar un objeto 3D como llave implica que ésta no es una función de fase pura, pero como discutimos en la sección anterior, el RCN causado por esta imperfección se puede mitigar, y en todo caso también está presente en las llaves generadas por difusores.

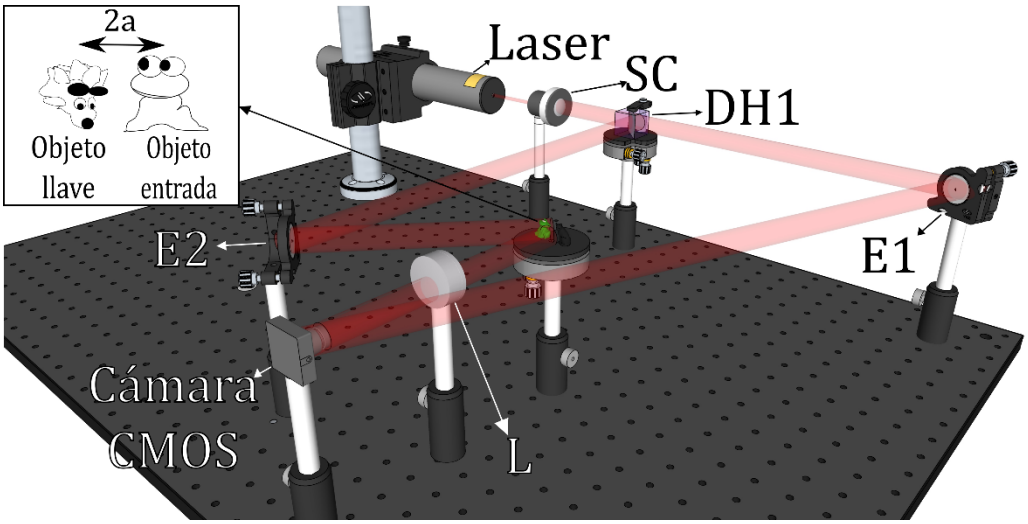

Figura 60: Esquema del criptosistema JTC 3D. E: espejo, DH: divisor de haz, SC: sistema de colimación, L: lente.

En la Figura 60 se muestra el esquema para la encriptación de objetos 3D con llave volumétrica. Este montaje es análogo al JTC de la sección 2.3, con la diferencia de que en el plano de entrada están ubicados los dos objetos físicamente en lugar de ser proyecciones en un modulador. Uno de los objetos servirá de llave y el otro será el objeto

a encriptar. Así pues, en el plano de la cámara CMOS se registra el JPS, y tras el proceso de filtrado, se obtiene el objeto encriptado dado por

$$E(v,w) = O_1(v,w)O^*{}_2(v,w) \tag{2.9.1}$$

donde $O_1(v,w), O_2(v,w)$ son las TF de los dos objetos $o_1(x,y), o_2(x,y)$. En este caso, suponemos que el objeto 2 será la llave y el 1 el que se está encriptando, sin embargo, seleccionando el complejo conjugado del objeto encriptado durante el filtrado es posible intercambiar los roles de los objetos.

Para obtener el objeto llave, simplemente se retira el objeto a encriptar del plano de entrada del sistema y se desbloquea el haz de referencia, registrando así un holograma de Fourier del cual se puede obtener la información de $O_2(v,w)$ tras un proceso de filtrado. En los resultados experimentales de esta sección se usó el esquema de la Figura 60 con una cámara CMOS EO-10012C de 3840×2748 de resolución y tamaño de pixel de $1.67\ \mu m \times 1.67\ \mu m$ como medio de registro y un láser DPSS de $532\ nm$ de longitud de onda con $300\ mW$ de potencia. Se usó una lente de $200\ mm$ de distancia focal. Las dimensiones máximas de los objetos son $18\ mm \times 24\ mm \times 16\ mm$. La separación $2a$ entre los objetos es de $35\ mm$.

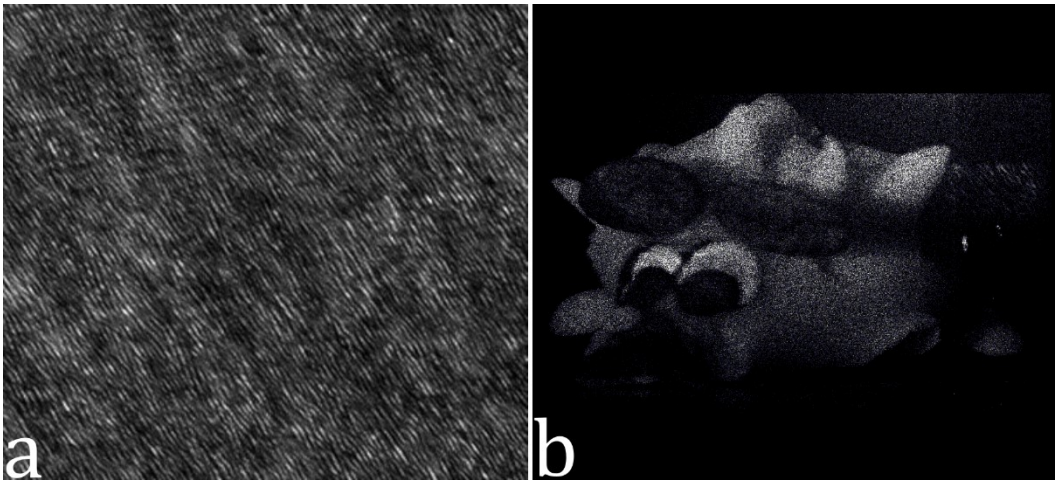

Figura 61: a) Holograma del objeto llave, b) reconstrucción filtrada de a).

En la Figura 61 se muestra el holograma del objeto llave y su reconstrucción tras aplicar el proceso de filtrado. Una vez conocemos $O_2(v,w)$ podemos usarlo para desencriptar la información contenida en la ecuación (2.9.1), tal que

$$d(v,w) = o_1(x,y) \otimes o^*{}_2(x,y) \otimes o_2(x,y) \tag{2.9.2}$$

La ecuación anterior se aproxima a $o_1(x,y)$, con la existencia del ruido que se discutió en la sección anterior. En este caso, ya que el objeto es real y no una proyección en un modulador, no se puede aplicar el PST. Asimismo, el uso de la modificación no lineal presenta grandes dificultades, ya que cualquier vibración del sistema entre la toma del JPS, del holograma de la llave y de la intensidad de la TF de la llave causará que los registros difieran, resultando en un aumento del ruido. Aunque este efecto está presente en el JTC convencional, al usar objetos 3D hay más grados de libertad en los cuales los objetos pueden vibrar.

Es por esto que en este caso se usa como única técnica de reducción de ruido la desencriptación sólo con la fase de la TF de la llave y la división por la ventana de Hamming durante el filtrado.

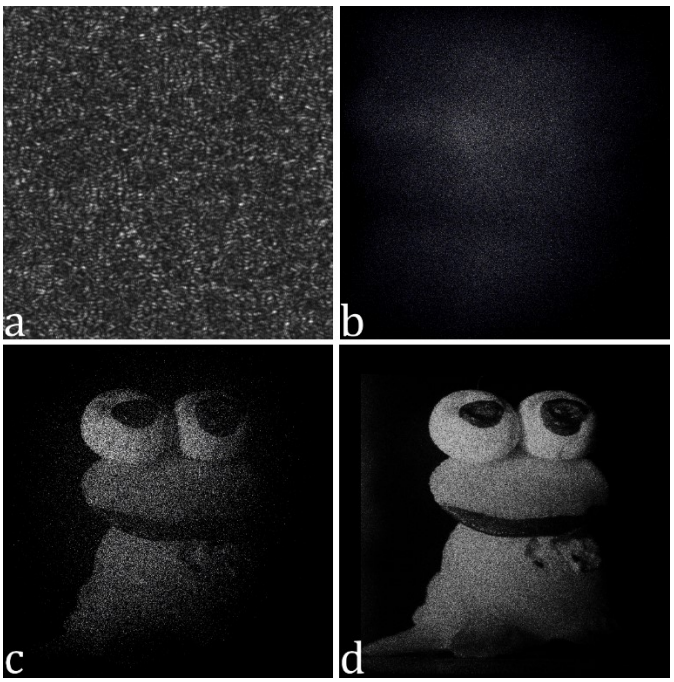

Figura 62: Encriptación de objetos 3D con llave volumétrica. a) JPS, b) TF del objeto encriptado, c) objeto desencriptado y d) reconstrucción del mismo objeto a partir de un holograma de Fourier.

En la Figura 62 se muestran los resultados de encriptación. Como se puede apreciar en la Figura 62.b, sin desencriptar no es posible reconocer ninguna característica del dato encriptado. Tras desencriptar con la llave de la Figura 61, obtenemos el objeto en la Figura 62.c. Para comparar la calidad del objeto recuperado, se muestra también la reconstrucción de un holograma de Fourier del mismo objeto. Como podemos esperar, al no ser la llave una máscara de fase aleatoria, el RCN causa una importante degradación, sin embargo, el dato desencriptado es reconocible.

En la encriptación de objetos 3D difusos no es necesario usar la división por la máscara de referencia descrita en la sección anterior, ya que la propia superficie del objeto se comporta como la máscara de fase que multiplica la entrada en el caso del JTC 2D, y por lo tanto no es fuente de ruido. Adicionalmente, ya que este sistema de encriptación es en esencia un sistema de holografía de Fourier fuera de eje, la profundidad axial de los objetos que se pueden encriptar adecuadamente es limitada. De la misma forma en la que implementamos este sistema, se puede construir un sistema de encriptación de datos 3D en el dominio de Fresnel o fraccional.

III. Compresión de datos holográficos

3.1. Introducción.

Ya habiendo expuesto los principios de la holografía digital y su extensión a la encriptación de datos ópticos, nos encontramos que en el trascurso de la investigación en el área cobra cada vez mayor importancia el estudio de técnicas de compresión de información holográfica.

Esto es debido a que las exigencias tanto de tamaño de pixel como de resolución para capturar adecuadamente un objeto con sistemas prácticos de holografía digital, hacen necesario el uso de cámaras de alta resolución, lo cual implica que los hologramas registrados tendrán un gran volumen de datos. Por ejemplo, para encriptar una imagen 2D de 400x400 pixeles como el resultado mostrado en la sección 2.3, usamos una cámara digital con resolución de 3840x2748. El JPS capturado requiere para su almacenamiento digital casi 66 veces más espacio que la imagen original.

Aunque este problema se puede obviar en algunos experimentos, ya que los computadores modernos tienen enorme capacidad de almacenamiento, cuando queremos procesar gran cantidad de datos o implementar sistemas prácticos de holografía digital, el uso eficiente de los recursos disponibles se convierte en una necesidad.

Existen dos tipos generales de métodos de compresión. Los métodos con perdida y sin perdida. Los métodos con perdida son aquellos en los cuales se logra compresión eliminando parte de la información a almacenar. En estos métodos se busca eliminar la máxima cantidad de información, pero de manera tal que la información restante continúe siendo inteligible. Ejemplo de métodos de compresión con perdida son usados

en los formatos mp3, mp4 y JPEG que se encuentran de manera generalizada en los sistemas digitales modernos. El único límite de estas técnicas consiste en el nivel de perdida que es tolerable para cierto tipo de información.

La compresión sin perdida, por otro lado, busca una nueva representación de la información que ocupe menos volumen sin eliminar los datos subyacentes. Estos métodos usualmente se basan en buscar periodicidades o redundancias en la información a comprimir y codificarlas en un diccionario. Ejemplos de estos métodos son la codificación Huffman [66] y LZ77 [67] usados en la compresión de archivos .zip.

El problema de la compresión de los datos holográficos ya ha sido sujeto de investigación, sin embargo, gran parte de ésta se centró en el uso de técnicas digitales, las cuales originalmente fueron diseñadas para la compresión de imágenes o textos, y demostraron tener una efectividad limitada cuando se aplicaron a los datos holográficos.

Por otro lado, la investigación de técnicas ópticas de compresión, las cuales operan con los mismos principios y limitaciones del sistema que genera la información que se desea comprimir, es una alternativa que puede ofrecer un rendimiento superior a las técnicas tradicionales, como mostraremos en este capítulo.

Así pues, expondremos algunos de los métodos digitales para la compresión de hologramas, y luego introduciremos dos técnicas opto-digitales de compresión novedosas, estudiando su rendimiento en comparación con métodos digitales.

3.2. Métodos digitales.

En esta sección discutiremos algunos de los métodos digitales de compresión. Para esto, primero debemos entender cómo se almacena la información registrada por una cámara digital.

Como ya hemos expuesto, una cámara digital es un arreglo de cierto número de pixeles. Sin entrar en los detalles finos del funcionamiento de estos pixeles, al recibir luz la cámara le asigna un valor binario a la intensidad detectada por cada pixel. Así, la imagen registrada es un arreglo de valores binarios, donde cada elemento corresponde a un pixel. Los valores binarios reportados por la cámara no son continuos, es decir, no representa el valor exacto de la intensidad del campo, si no que están cuantizados en un número finito de niveles. Dependiendo de la sensibilidad de la cámara y su construcción

electrónica, el valor binario que representa la intensidad en cada pixel tendrá un límite de tamaño en bits. A esto se le denomina profundidad de bit.

Una cámara convencional tiene una profundidad de 8 bits, es decir, es capaz de detectar 256 niveles de intensidad distintos. Cámaras más sofisticadas pueden tener profundidades de bit de 10, 12 y hasta 16 bits. La cantidad de niveles de intensidad diferentes que se pueden medir con una cámara es dada por 2^B, donde B es la profundidad de bit.

Así pues, la imagen registrada por una cámara va a tener un tamaño total en bits igual al número de pixeles multiplicado por la profundidad de bit, así

$$V = N \times M \times B \tag{3.2.1}$$

donde V es el volumen de los datos en bits, N y M son el número de pixeles horizontales y verticales de la cámara y B es la profundidad de bit. Ahora bien, una vez registrado un holograma, este es reconstruido, con una transformada de Fourier o de Fresnel según el caso. Aunque la cámara registra una intensidad, su TF será un valor complejo, y ocupara el doble de volumen, ya que se requiere almacenar información de amplitud y de fase para cada pixel. Teniendo en cuenta esto, la forma más directa de compresión se obtiene logrando una reducción o en el número de pixeles a almacenar o en la profundidad de bit con la que son almacenadas.

Afortunadamente, ya hemos expuesto un método efectivo para reducir significativamente el número de pixeles que se tienen que almacenar de un holograma o JPS: el filtrado. Tras realizar la TF del holograma, nos quedamos con la información correspondiente al campo óptico del objeto o al dato encriptado. Si recordamos las condiciones para el registro de hologramas digitales, esta información podrá tener como máximo una extensión menor o igual a la mitad de espacio total del holograma. Esto implica que, en el peor de los casos, tenemos que el volumen del campo óptico o dato encriptado será

$$V_f = \frac{2 \times N \times M \times B}{4} \tag{3.2.2}$$

Donde el 2 en el numerador aparece debido a que tras el filtrado se obtienen datos complejos. Así, el filtrado permite reducir el volumen de los hologramas y datos encriptados de manera sencilla y sin perder información relevante para la

reconstrucción. Teniendo en cuenta esto, una forma de evaluar la efectividad del filtrado para reducción de volumen es el denominado factor de compresión R_c, definido como

$$R_C = \frac{V_i}{V_f} \tag{3.2.3}$$

con V_i el volumen en bits del dato antes de comprimir y V_f después. En el caso descrito anteriormente, se logra un factor de compresión de 2. Para tener una referencia, los videos en resolución "full HD" (correspondientes a 1920x1080 pixeles), suelen ser comprimidos con un factor de compresión de 50, usando una combinación de algoritmos con perdida y sin perdida.

Ahora bien, si deseamos mayor compresión sin afectar la reconstrucción, es posible intentar con algoritmos ya usados con este propósito. Naughton *et al* [68] realizaron un estudio extensivo donde probaron distintos tipos de compresión aplicados a datos holográficos. En su trabajo, encontraron que los algoritmos de compresión sin perdida presentaban un rendimiento muy bajo, logrando en la mayoría de los casos factores de compresión de 1.3. Esto se debe a que los datos holográficos de objetos difusos son altamente aleatorios, y no es posible para los algoritmos sin perdida encontrar redundancias o periodicidades en la información de forma confiable.

En este sentido, si queremos altos factores de compresión, debemos recurrir a métodos con perdida, por ejemplo, descartando la información de amplitud como se expuso en la sección 1.8. Esto nos permite reducir el volumen de los datos filtrados a la mitad. Otra forma directa de compresión consiste en reducir la profundidad de bit con la que se almacena la información digitalmente. Esta posibilidad fue estudiada durante los primeros años de la investigación en holografía digital y computacional, ya que las computadoras de la época tenían limitaciones extremas en cuanto a capacidad de memoria. Goodman & Silvestri, mostraron por primera vez los efectos de cuantización en la fase de la TF de un objeto [69]. Trabajos posteriores mostraron que guardar la fase con menos de 4 bits causa un aumento del error en la reconstrucción, con la aparición de ruido de cuantización, imágenes falsas y otros artefactos [70–73].

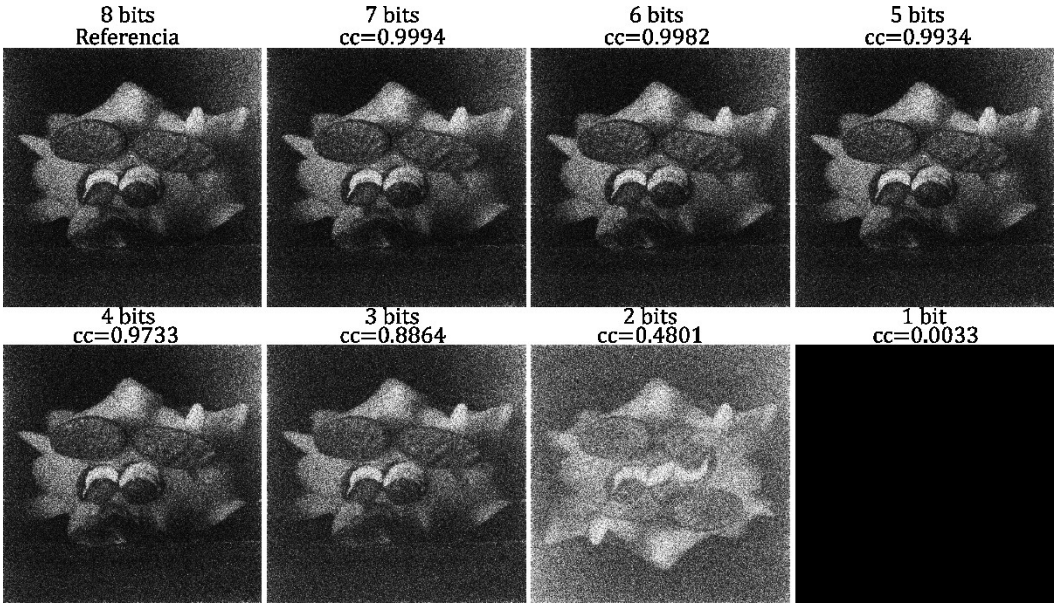

Figura 63: Efectos de la reducción de la profundidad de bit en la reconstrucción de un objeto con sólo fase. (cc: coeficiente de correlación)

En la Figura 63 se muestra el efecto de reconstruir un objeto a partir de la fase del campo óptico filtrado de un holograma de Fourier, cuando se reduce la profundidad de bit. El holograma original fue tomado con el esquema de la sección 1.3, usando una cámara EO-10012C de 3840 x 2748 pixeles de resolución con una profundidad de bit de 8. En la figura incluimos el coeficiente de correlación de la reconstrucción con reducción en la profundidad de bit con la referencia obtenida con 8 bits. Estos coeficientes muestran cómo la perdida entre 8 y 4 bits es relativamente pequeña, volviéndose mayor en 3 bits y luego extrema por debajo de este valor.

De esta manera, usar 4 bits para almacenar los campos ópticos filtrados es, en la mayoría de los casos, un buen compromiso entre la calidad de la reconstrucción y la reducción de volumen, logrando así un factor de compresión de 2 con respecto al campo óptico original con profundidad de 8 bits.

Ninguna de las operaciones hasta ahora propuestas, con excepción del filtrado, nos permite obtener factores de compresión mayores a 2. La última opción directa para lograr factores mayores es disminuir el número de pixeles en la imagen. Una opción para lograr esto consiste en realizar un escalado digital del campo óptico, el cual consiste en volver a muestrear el campo como si fuera registrado por un sensor con mayor tamaño de pixel, por ejemplo, asignando a un nuevo pixel del campo el valor promedio de 4 pixeles adyacentes. Este y otro tipo de algoritmos de escalado están optimizados para

imágenes, y como demostraron Naughton *et al* [68], causan gran degradación en la reconstrucción, incluso cuando el nivel de escalado es mínimo.

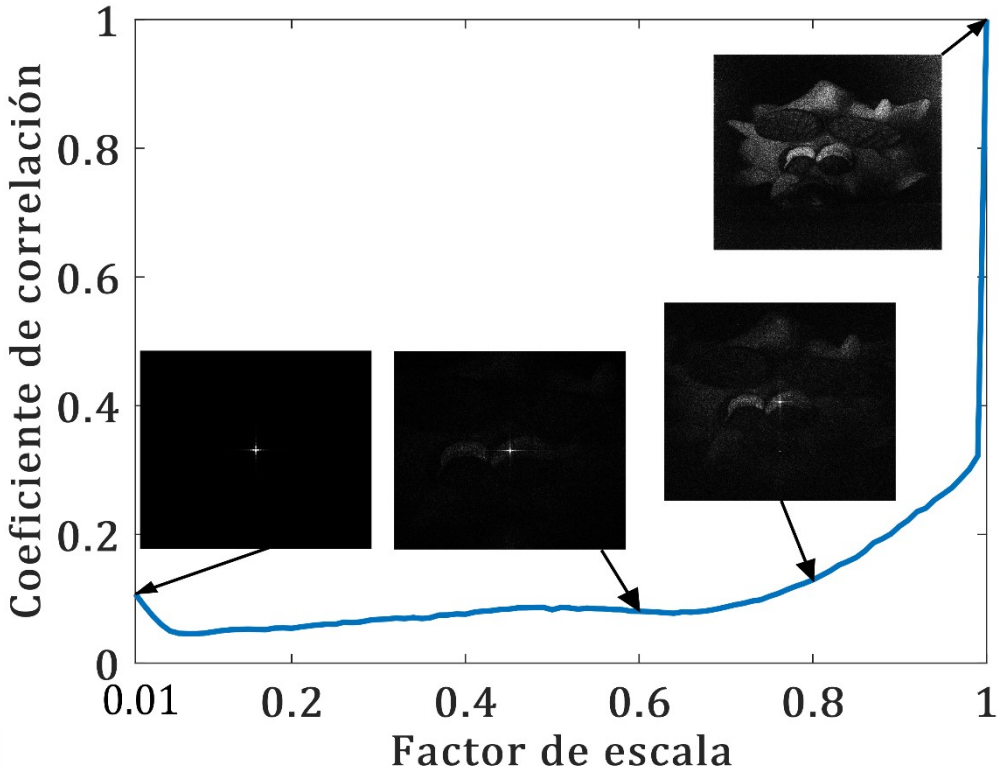

Figura 64: Coeficiente de correlación de un objeto reconstruido a partir de campos ópticos escalados digitalmente.

En la Figura 64 se muestra la curva del coeficiente de correlación de un objeto reconstruido a partir de campos ópticos escalados digitalmente, usando el objeto reconstruido sin escalado como referencia. El factor de escala determina la reducción en el número de pixeles con respecto al dato original. Como se puede apreciar, el coeficiente de correlación y la calidad de la reconstrucción caen rápidamente al aplicar el escalado, confirmando los resultados de Naughton *et al*.

Así pues, los métodos directos de compresión digital no nos permiten obtener grandes reducciones de volumen de datos holográficos, a pesar de que, para imágenes, videos y música, factores de compresión de 20 a 50 son alcanzados rutinariamente.

Para lograr altos grados de compresión, los algoritmos más sofisticados hacen uso de técnicas de análisis espectral, en las cuales se realizan transformadas de distintos tipos sobre los datos, de manera tal que sean más densas en información en la nueva representación y así reducir la cantidad de pixeles que se deben guardar. El filtrado que

hemos empleado a lo largo de este trabajo es una operación de este tipo, sin embargo, obtener mayor compresión en información holográfica de objetos difusos es difícil, ya que el campo óptico está distribuido por todo el espacio. Para este fin, precisamente, requerimos usar objetos difusos para un registro adecuado, como explicamos en la sección 1.4. Así, nos encontramos con que los requisitos para el registro holográfico y los requisitos para obtener altos grados de compresión son contradictorios. En uno requerimos una transformada cuya energía este bien distribuida en el espacio, y en el otro caso que este lo más localizada posible.

Otro tipo de métodos de compresión, como el usado por el algoritmo JPEG [74] (del inglés "joint photographic experts group"), divide los datos en bloques, y aplica una transformación a cada bloque, cuantizando los coeficientes de la transformada resultante. En imágenes, este método es muy eficiente, pues un bloque de pixeles puede tener valores muy similares, permitiendo un alto grado de compresión. En un holograma, por otro lado, tenemos un diagrama de speckle donde todos los bloques van a presentar variaciones aleatorias de sus valores. Así, la compresión posible en todos los bloques va a ser muy limitada. De hecho, ya Shahnaz *et al* [75] mostraron que la presencia de ruido aleatorio implica una reducción en la efectividad de la compresión JPEG. Debido a las dificultades aquí expuestas para la compresión de hologramas por medios digitales, ahora procederemos a explorar algunas alternativas ópticas.

3.3. Escalado óptico.

Con Trejos *et al* [76], presentamos una alternativa opto-digital a los algoritmos clásicos de compresión. La idea detrás de esta propuesta es realizar el escalado de un dato encriptado usando una lente convergente, en lugar de un algoritmo digital, y de esta manera evitar las interpolaciones que realizan los métodos digitales y mantener la integridad de la información.

En nuestra propuesta, usamos el esquema de la sección 2.3 para registrar el JPS de un dato. A este JPS se le aplica el proceso de filtrado, obteniendo el objeto encriptado. Tras realizar este proceso, obtenemos un factor de compresión dado por

$$R_{filt} = \frac{N \times M \times 8}{2 \times N_f \times M_f \times 8} \tag{3.3.1}$$

Donde N, M es el número de pixeles del JPS en la dirección vertical y horizontal, respectivamente, y N_f, M_f el número de pixeles del objeto encriptado tras el filtrado. Luego de realizar el filtrado, simulamos la formación de imagen por una lente convergente de distancia focal f, con el dato encriptado ubicado en el plano de entrada a una distancia d_1 de la misma, como se muestra en la Figura 65. La imagen del dato encriptado se forma a una distancia d_2, y tendrá las dimensiones del dato filtrado escaladas por la magnificación del sistema [77], dada por

$$E = \frac{f}{f - d_1} \tag{3.3.2}$$

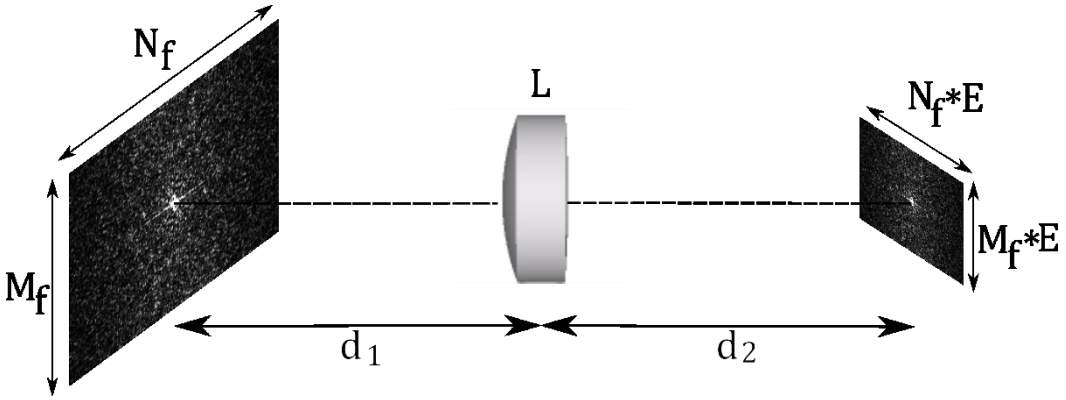

Figura 65: Esquema para el escalado opto-digital.

Tras realizar este escalado, se obtiene un factor de compresión dado por

$$R_E = \frac{2 \times N_f \times M_f \times 8}{2 \times N_f \times M_f \times E^2 \times 8} = \frac{1}{E^2} \tag{3.3.3}$$

Para lograr compresión es necesario que E sea menor que 1, lo que implica que d_1 debe ser mayor que $2f$. Combinando el filtrado y el escalado óptico, obtenemos finalmente un factor de compresión dado por

$$R_T = \frac{N \times M \times 8}{2 \times N_f \times M_f \times E^2 \times 8} \tag{3.3.4}$$

Una vez se tiene el objeto encriptado comprimido, el proceso de escalado debe deshacerse antes de poder desencriptarlo satisfactoriamente. Dado que durante el escalado hay una pérdida de información, ya que se está reduciendo el número de pixeles respecto a los datos originales, al revertirlo y desencriptar se puede apreciar una

degradación en el resultado, comparado con el objeto obtenido de un dato encriptado sin comprimir. No obstante, esta degradación es mucho menor que la que causa el escalado digital.

Una ventaja de este método de compresión radica en que se pueden procesar múltiples datos simultáneamente, usando el multiplexado. Para lograr esto, se realiza un arreglo de todos los datos filtrados que se van a encriptar y se lo ubica en el plano de entrada de la lente que realiza el escalado.

Para demostrar la efectividad de nuestra propuesta, encriptamos 16 objetos usando el sistema de la sección 2.3, con una cámara CCD PULNIX TM7603 con 640×480 pixeles de resolución, tamaño de pixel de 9 μm y 8 bits de profundidad por pixel. Cada JPS registrado con este sistema tiene un volumen de 300 kilobytes (KB) (1 KB= 1024 bytes, 1 byte=8 bits), para un volumen total de 4.69 megabytes (MB, 1 MB = 1024 KB), contando los 16 registros.

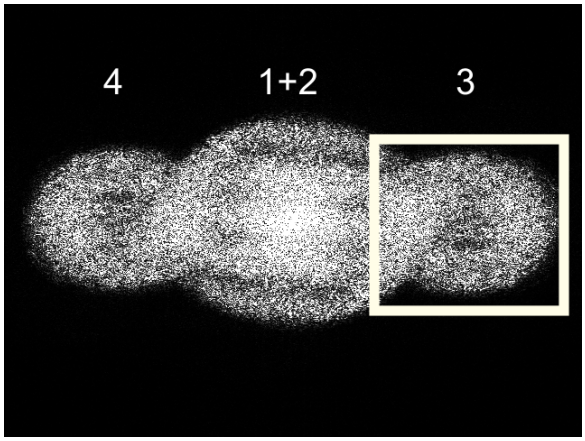

Figura 66: Filtrado del JPS.

Cada JPS es luego sometido al proceso de filtrado. En la Figura 66 se muestra el área filtrada de la TF de uno de los JPS, correspondiente al cuadro blanco. Los números representan los distintos términos de la TF del JPS, siendo 1 y 2 el orden central, 3 el dato encriptado y 4 su complejo conjugado. El área filtrada tiene 177×198 pixeles, y por lo tanto ocupa un volumen de 68.45 KB. Esta área fue igual para los 16 objetos, lo que da un volumen total de 1.07 MB.

Luego, ordenamos los 16 datos escalados en un arreglo cuadrado, y aplicamos el escalado óptico. Usando una magnificación de 0.5, obtenemos un volumen final de los

datos de 0.27 MB, correspondiente a un factor de compresión total de 17.53 y a una reducción del 94.24% respecto al volumen de los JPS iniciales.

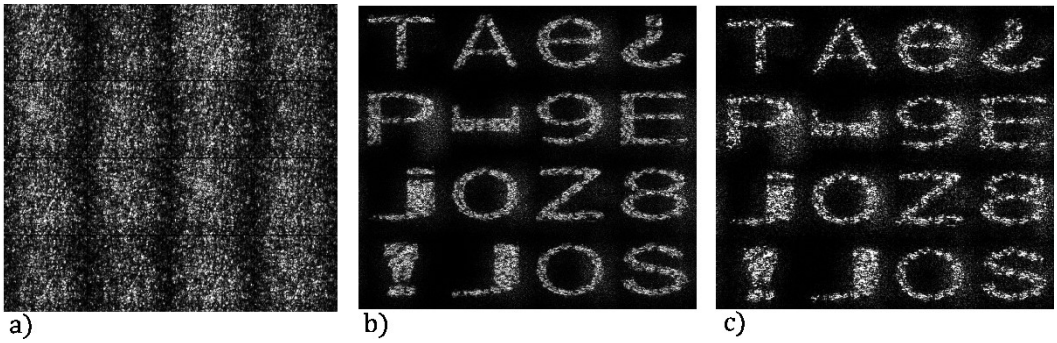

Figura 67: a) arreglo de 16 objetos filtrados, b) desencriptación de a) sin escalado óptico y c) con escalado óptico correspondiente a una magnificación de 0.5.

En la Figura 67 se muestra el resultado de desencriptar el arreglo de 16 datos encriptados sin escalado (Figura 67.b) y luego de escalar con una magnificación de 0.5 (Figura 67.c). Como se puede apreciar, el escalado causa un aumento en el tamaño del speckle en los objetos desencriptados, pero estos se mantienen reconocibles. En estos resultados no se aplicó ninguna de las técnicas de reducción de ruido de la sección 2.8.

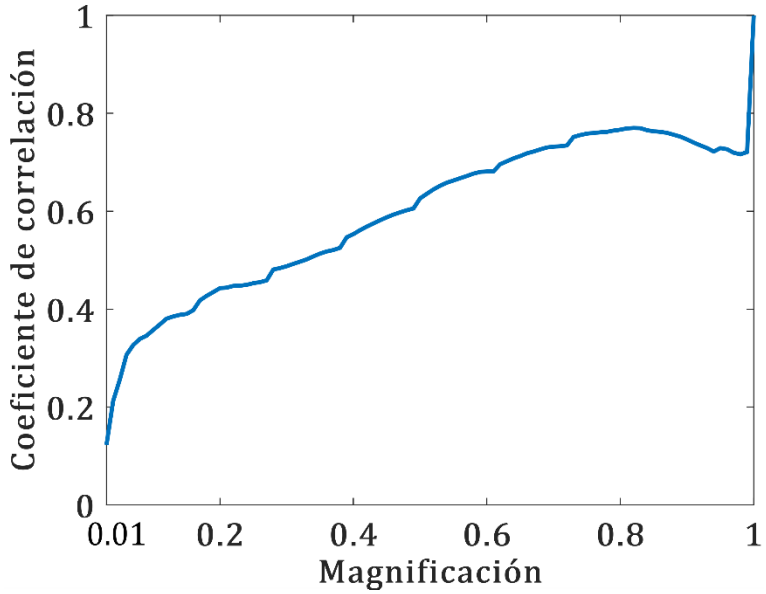

Figura 68: Coeficiente de correlacion de arreglos de 16 objetos desencriptados tras ser comprimidos con distinta magnificación.

En la Figura 68 se muestra como varía el coeficiente de correlación al desencriptar los arreglos comprimidos con distintos grados de magnificación. Al igual que en el caso del escalado digital que se muestra en la Figura 64, hay una disminución del coeficiente de correlación al aplicar el escalado óptico, sin embargo, en este caso la disminución es debida a que el paso por una lente virtual introduce cambios de fase en el dato

comprimido que aumenta el ruido al desencriptar. Como mostraremos a continuación, este efecto no aparece al comprimir datos holográficos sin encriptación. Para mostrar esto y realizar un análisis más exhaustivo del efecto del escalado, en Velez *et al* [78] aplicamos la propuesta a hologramas de objetos 3D. En este trabajo, comparamos el rendimiento del escalado óptico cuando es aplicado a la fase y a la amplitud de un objeto, y comparamos su desempeño con el standard JPEG de compresión.

Para ello registramos la información de un objeto 3D usando el esquema de la sección 1.3 con una cámara EO-10012C de 3840 x 2748 pixeles de resolución con una profundidad de bit de 8. La fuente de iluminación fue un láser DPSS de 532 nm de longitud de onda y 300mW de potencia. Para realizar la TF ópticamente se usó una lente de 200 mm de distancia focal. El ángulo entre el haz de referencia y el haz objeto fue de 5º.

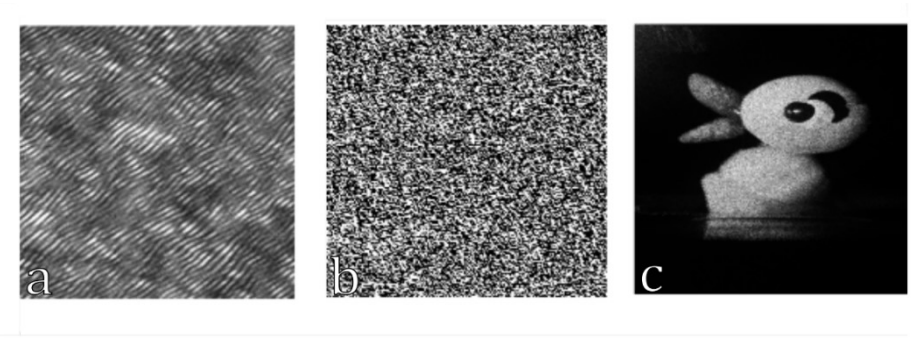

Figura 69: a) holograma de Fourier, b) campo óptico filtrado, y c) objeto reconstruido.

En Figura 69 se muestra el holograma registrado, el campo óptico filtrado y el objeto reconstruido que usaremos para probar el escalado óptico y compararlo con la compresión JPEG. El holograma registrado tiene un volumen de 10.06 MB. El área filtrada correspondiente al campo óptico de la TF del objeto es de 940x940 pixeles, con un volumen de 1726 KB.

A continuación, calculamos el coeficiente de correlación entre el objeto reconstruido del campo óptico sin compresión y el reconstruido de campos ópticos comprimidos con escalado óptico y con el standard JPEG, usando distintos valores de magnificación y factor de calidad (QF por las siglas en ingles de “quality factor”).

El factor de calidad es una variable del standard JPEG que permite controlar el grado de compresión que se aplica. Este factor es un numero entero entre 1 y 100 que determina el nivel de cuantización de los coeficientes de la transformación coseno por bloques que

realiza el standard, donde 100 equivale a no realizar ninguna cuantización y 1 corresponde a la máxima cuantización posible.

Debido a que la magnificación y el factor de calidad son variables que afectan de distinta forma el nivel de compresión logrado por cada método, el coeficiente de correlación se graficó respecto a la diferencia entre el volumen de la información antes y después de la compresión, tal que

$$\Delta V = V_R - V_C \tag{3.3.5}$$

Donde V_R es el volumen del campo óptico sin comprimir y V_C es el volumen del campo óptico comprimido.

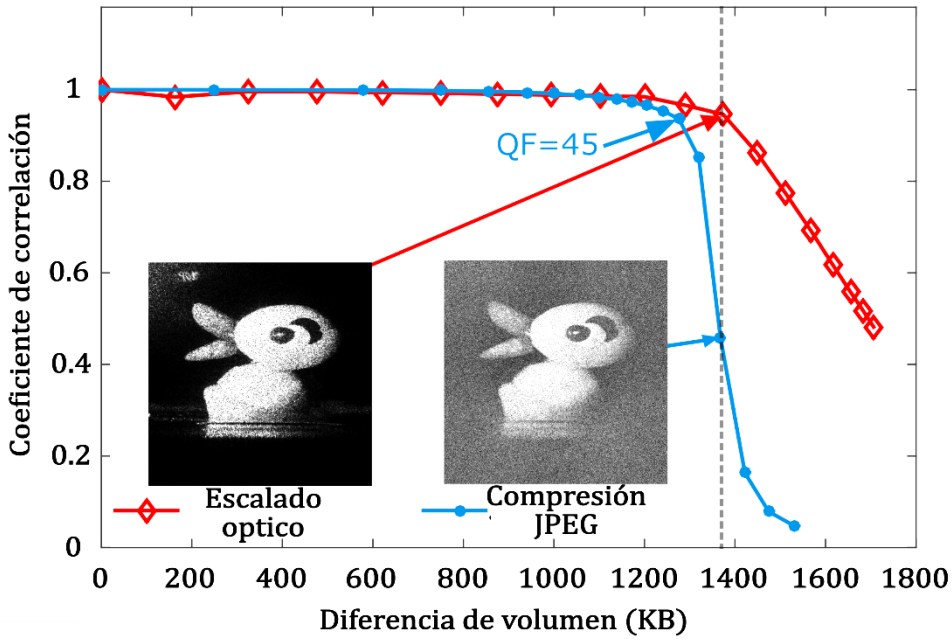

Figura 70: Coeficiente de correlación entre el objeto reconstruido de un campo óptico sin compresión y de un campo óptico comprimido con escalado óptico y JPEG en función de la diferencia de volumen.

En la Figura 70 se muestra la curva del coeficiente de correlación mencionada. Cada punto de las líneas corresponde a una disminución de 5 en el factor de calidad para el JPEG y de 0.05 en la magnificación. En el caso de la compresión JPEG, se logra un coeficiente de correlación cercano a 1 hasta un factor de calidad de 45. Al disminuir el factor de calidad aún más, el objeto recuperado sufre una rápida degradación. En el caso del escalado óptico, la degradación es mucho más suave. En las imágenes insertadas en la gráfica se puede apreciar el resultado reconstruido de los campos ópticos con el mismo

factor de compresión, equivalente a una diferencia de volumen de 1380 KB. En el caso del escalado óptico, la calidad de la reconstrucción es significativamente superior. Así pues, para obtener altos factores de compresión el escalado óptico ofrece mayor calidad que el JPEG para su aplicación a datos holográficos.

A continuación, evaluaremos el desempeño de los métodos de compresión expuestos cuando son aplicados a la fase y a la amplitud del campo óptico por separado.

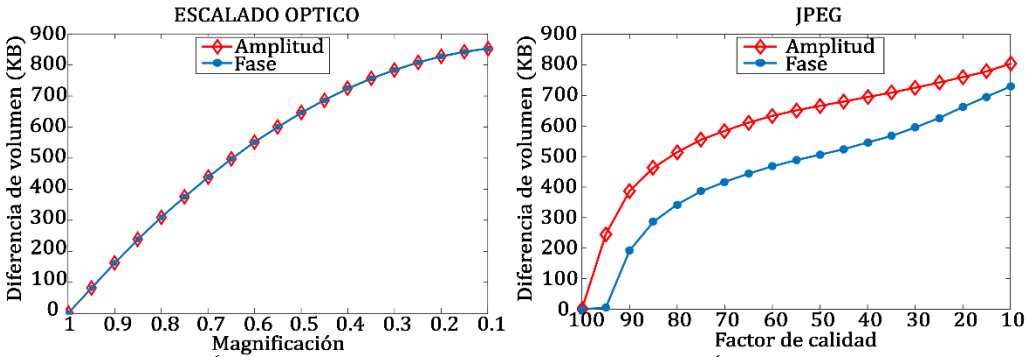

Figura 71: Diferencia de volumen de la fase y la amplitud de los datos comprimidos en función de la magnificación con escalado óptico y el factor de calidad con JPEG.

En la Figura 71 se muestra el resultado de este análisis. En el caso de la compresión con escalado óptico, se obtiene la misma diferencia de volumen para la fase y la amplitud para todos los valores de magnificación. En el caso de la compresión JPEG, esto no ocurre. Para todos los valores de factor de calidad, se obtiene menos diferencia de volumen para la fase que para la amplitud. Este efecto concuerda con las observaciones de Shahnaz *et al* [75], ya que la amplitud presenta variaciones suaves y continuas que son fáciles de comprimir para el algoritmo JPEG, mientras que la fase presenta discontinuidades correspondientes a saltos entre los valores $\pi, -\pi$ debido al fenómeno de envolvimiento de la fase, las cuales hacen que se comporte de forma similar a un ruido aleatorio, disminuyendo la efectividad del método.

Si tenemos en cuenta que la fase es la portadora de gran parte de la información del objeto, como se expuso en la sección 1.8, el problema de compresión de información holográfica se puede reducir en última instancia al problema de compresión de información de fase. Como pudimos verificar, el estándar JPEG y gran parte de los métodos de cuantización espectral con transformaciones coseno, wavelet, etc, no fueron diseñados para el procesamiento de información casi aleatoria como lo es la fase de objetos difusos, si no para imágenes con variaciones suaves de intensidad. Así pues, el escalado óptico ofrece una alternativa con mejor rendimiento para este propósito, y

muestra que los métodos ópticos pueden ser superiores a los algoritmos tradicionales de compresión, en cuanto al tratamiento de información holográfica se refiere.

3.4. Muestreo aleatorio.

En la sección 1.6, se expuso el multiplexado, como una forma de combinar la información de múltiples hologramas para construir escenas extendidas, superando así las limitaciones del sistema de registro holográfico. Uno de los requisitos que pusimos en la técnica de multiplexado expuesta, fue que los distintos objetos no se superpusieran en el plano de reconstrucción, ya que de lo contrario no es posible diferenciar la información de cada uno.

Sin embargo, el multiplexado con superposición es una forma de compresión: en lugar de reducir el número de pixeles del campo óptico a guardar, se guardan múltiples campos ópticos en el volumen ocupado por uno solo, logrando así un factor de compresión igual al número de campos multiplexados. Para poder aprovechar esta forma de compresión sin el problema de la superposición, en Velez *et al* [79] propusimos una técnica basada en el muestreo de los campos ópticos con máscaras binarias aleatorias. El uso de estas mascaras permite hacer reversible el proceso de multiplexado sin necesidad de garantizar que los objetos no se superpongan.

Para justificar nuestra propuesta, nos remontamos a la sección 2.2, donde dedujimos que la condición para la reconstrucción adecuada de un objeto con un correlador óptico es

$$o(x,y) \otimes f^{*}(x,y) \approx o(x,y) \qquad (3.4.1)$$

Donde $o(x,y)$ es el objeto por reconstruir, y $f^{*}(x,y)$ es una función cualquiera que cumpla la condición anterior, para lo cual debe ser aproximadamente igual a una delta de Dirac. Entre las funciones que tienen esta característica, encontramos a la transformada de Fourier de una máscara binaria aleatoria. Estas mascaras son funciones bidimensionales donde cada punto tiene asignado aleatoriamente un valor de 1 o 0. Al multiplicar la TF del objeto por una máscara binaria aleatoria y al intentar reconstruir el producto resultante se obtiene

$$o(x,y) \otimes TF(B(v,w)) \qquad (3.4.2)$$

donde $B(v,w)$ es la máscara binaria aleatoria. Que tanto se aproxime la reconstrucción de la ecuación anterior al caso ideal, dependerá del porcentaje de puntos con valor 1 respecto a los puntos con valor 0 en la máscara. En el caso de que todos los puntos valgan 1, se reduce al caso de la reconstrucción holográfica convencional, de lo contrario, la calidad de la reconstrucción dependerá del porcentaje de puntos con valor 1 en la máscara binaria.

Esta propiedad de las máscaras binarias aleatorias hizo que Davis & Cottrel [80] propusieran su uso para multiplexar filtros de fase. En lugar de sumar dos filtros, lo que puede causar efectos indeseados de superposición, tal y como ocurre con los hologramas, multiplicaron las TFI de los filtros con máscaras binarias ortogonales, es decir, que los puntos donde una de las máscaras tiene valor 1 corresponde a los puntos donde la otra tiene valor 0. Aunque el uso de estas mascaras disminuía la relación señal ruido de los filtros, permitía eliminar los efectos indeseados causados por la superposición.

Al muestrear campos ópticos con máscaras binarias aleatorias, encontramos que, en efecto, mientras menos pixeles "blancos" (con valor 1) tenga la máscara, mayor será la degradación del objeto tras la reconstrucción, sin embargo, podemos usar un método de "rellenado" (padding en inglés) para mitigar este efecto. El rellenado aumenta el número de pixeles del campo óptico, resultando en un mayor volumen, lo que parece contraproducente si nuestro deseo es la compresión de datos, pero como mostraremos, el rellenado combinado con el muestreo con máscaras aleatorias permite un control granular tanto del factor de compresión como de la calidad de la reconstrucción de los objetos.

El proceso de rellenado consiste en realizar la TF del campo óptico filtrado, y luego añadirle un determinado número de pixeles con valor 0 a sus bordes. Tras realizar este proceso, se realiza una TFI, obteniendo el campo óptico filtrado y con relleno. En los resultados y análisis de esta sección, los pixeles se añaden en igual proporción en la dirección vertical y horizontal. Este método es similar al usado para ecualizar los tamaños de pixel en holografía digital a color [12].

Para probar el efecto de las máscaras binarias aleatorias y del relleno, usamos un campo óptico filtrado de 1200x1200 pixeles, registrado como un holograma de Fourier

de un objeto 3D. Luego se multiplico este campo con máscaras binarias con un decreciente porcentaje de pixeles blancos, calculando el coeficiente de correlación entre el objeto reconstruido del campo óptico original y del campo óptico muestreado. El mismo procedimiento se realizó con el campo óptico rellenado hasta un tamaño de 3000x3000 pixeles.

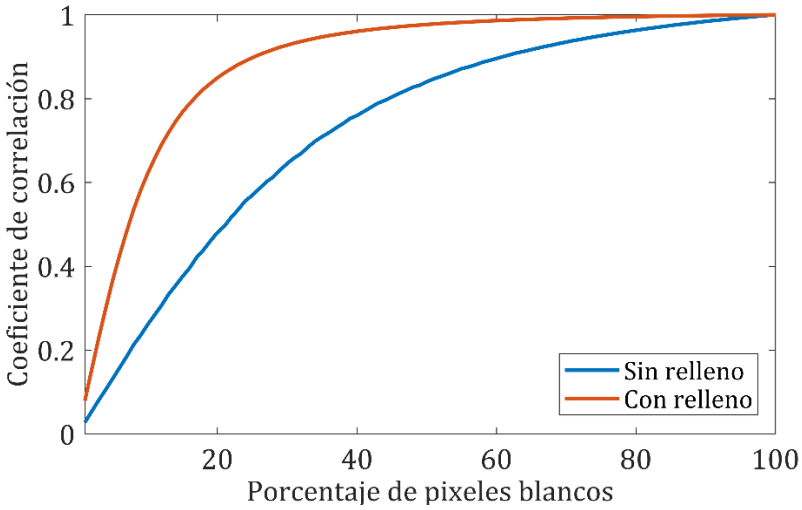

Figura 72: Coeficiente de correlación entre el objeto reconstruido a partir de un campo óptico muestreado con máscaras binarias aleatorias y de un campo óptico sin muestrear.

En la Figura 72 vemos como el coeficiente de correlación disminuye conforme se reduce el porcentaje de pixeles blancos en la máscara binaria aleatoria usada. Al usar el relleno, se incrementa la redundancia de los datos, lo que permite usar máscaras con un menor porcentaje de pixeles blancos manteniendo un coeficiente de correlación superior al caso sin relleno.

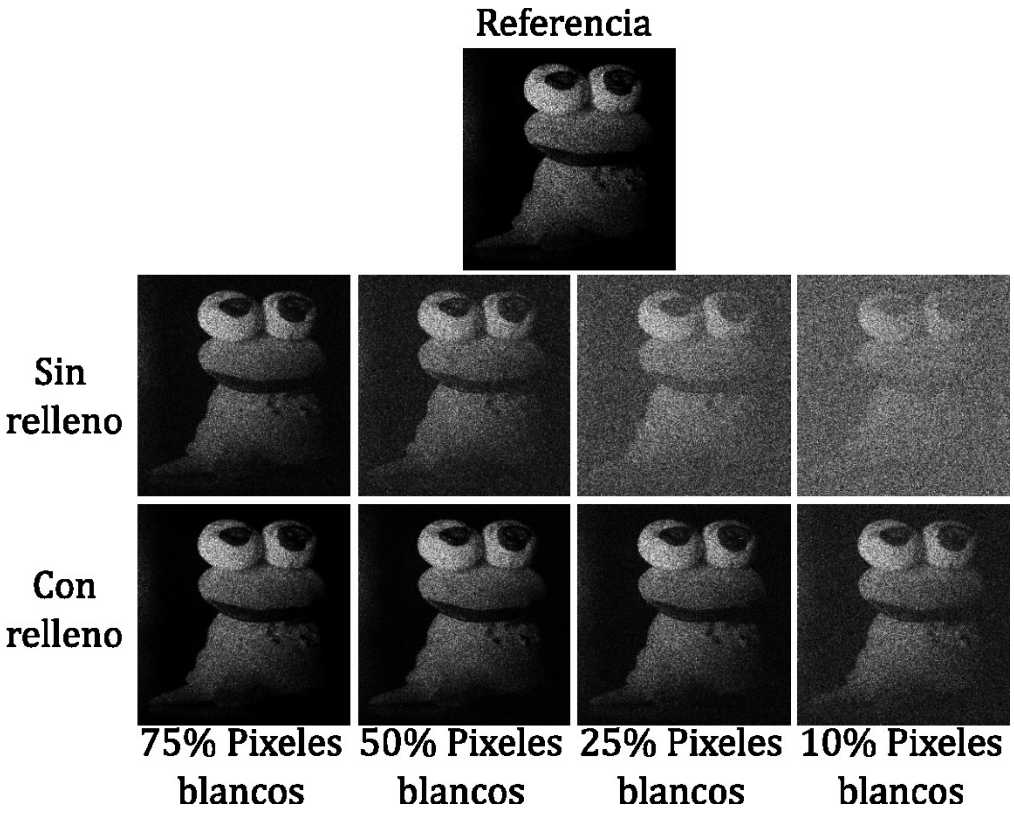

Figura 73: Objeto reconstruido de un campo óptico muestreado con diferentes máscaras binarias aleatorias.

En la Figura 73 se muestran los objetos reconstruidos a partir de los campos ópticos muestreados. En el caso sin relleno, el objeto presenta una degradación considerable en el resultado donde se usó la máscara con 25% de pixeles blancos, mientras que en el resultado con relleno el objeto presenta poco ruido visible incluso cuando se usa una máscara con 10% de pixeles blancos. Este resultado confirma la tendencia de la Figura 72.

Los resultados de esta sección fueron obtenidos procesando hologramas de Fourier registrados usando el esquema de la sección 1.3, con una cámara EO-10012C de 3840 x 2748 pixeles de resolución con una profundidad de bit de 8. La fuente de iluminación fue un láser DPSS de 532 nm de longitud de onda y 300mW de potencia. Para realizar la TF ópticamente se usó una lente de 200 mm de distancia focal. El ángulo entre el haz de referencia y el haz objeto fue de 5º.

Una vez determinamos el efecto del muestreo con máscaras aleatorias y el relleno en la reconstrucción de los objetos, podemos proceder a la compresión de datos sumando los campos ópticos de varios objetos, muestreados con máscaras binarias aleatorias que sean ortogonales entre sí, es decir, que dos mascaras no muestreen el mismo pixel. De

esta manera, se pueden sumar los campos muestreados, y no hay superposición entre ellos, a pesar de que ocupan una matriz con el mismo número de pixeles.

Para reconstruir un objeto determinado contenido en el multiplexado, se multiplica el mismo por la máscara binaria con la que fue muestreado el campo correspondiente, y se realiza el proceso de reconstrucción. De esta manera, podemos seleccionar a voluntad los objetos a reconstruir, evitando que todos aparezcan superpuestos en el plano de reconstrucción.

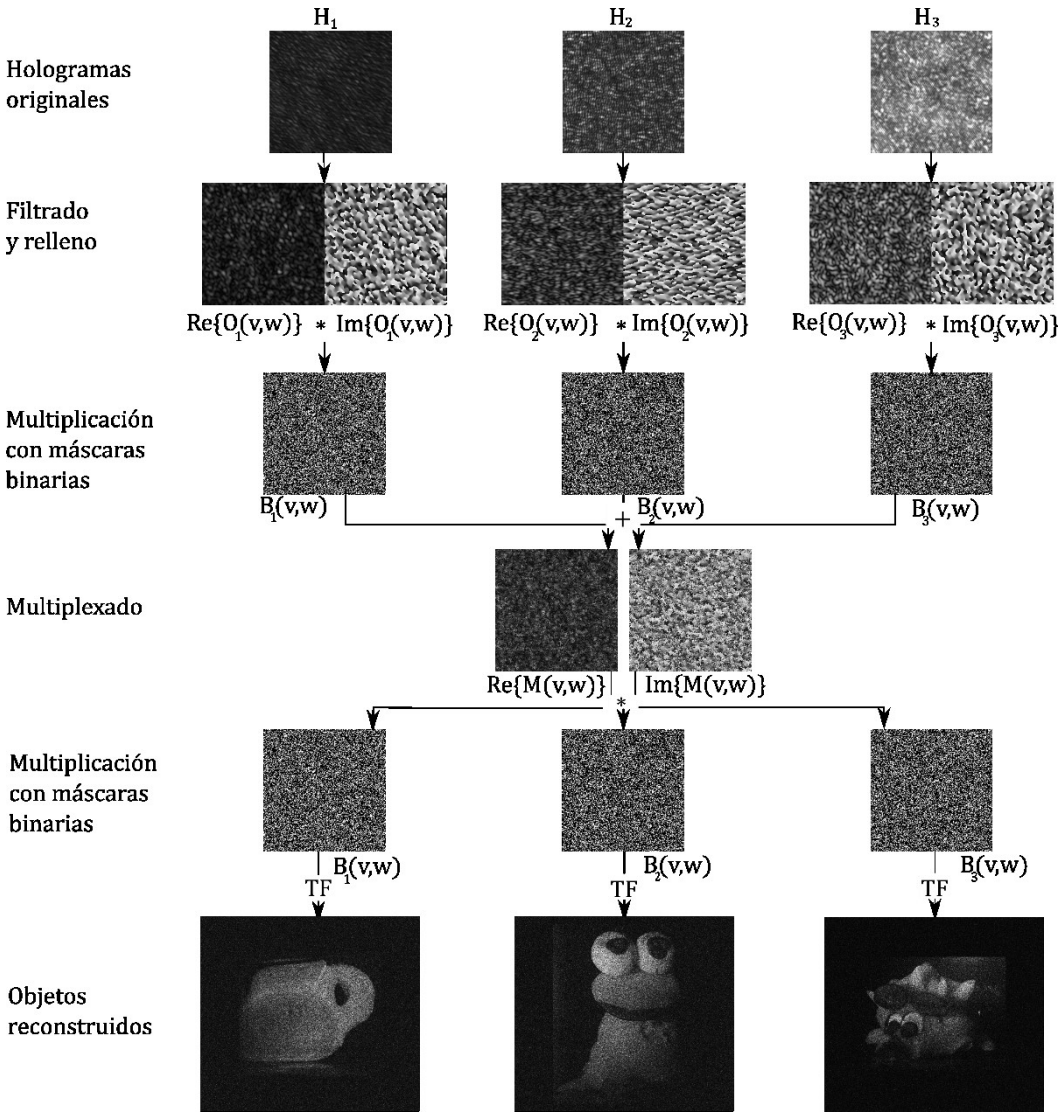

Figura 74: Diagrama de flujo del proceso de multiplexado con máscaras binarias aleatorias.

En la Figura 74 se muestra un diagrama de flujo del proceso de multiplexado propuesto para tres objetos, muestreados con 33% de pixeles blancos cada uno. Los campos ópticos filtrados tenían tamaño de 1200x1200 y fueron rellenados hasta un tamaño de 1800x1800 pixeles.

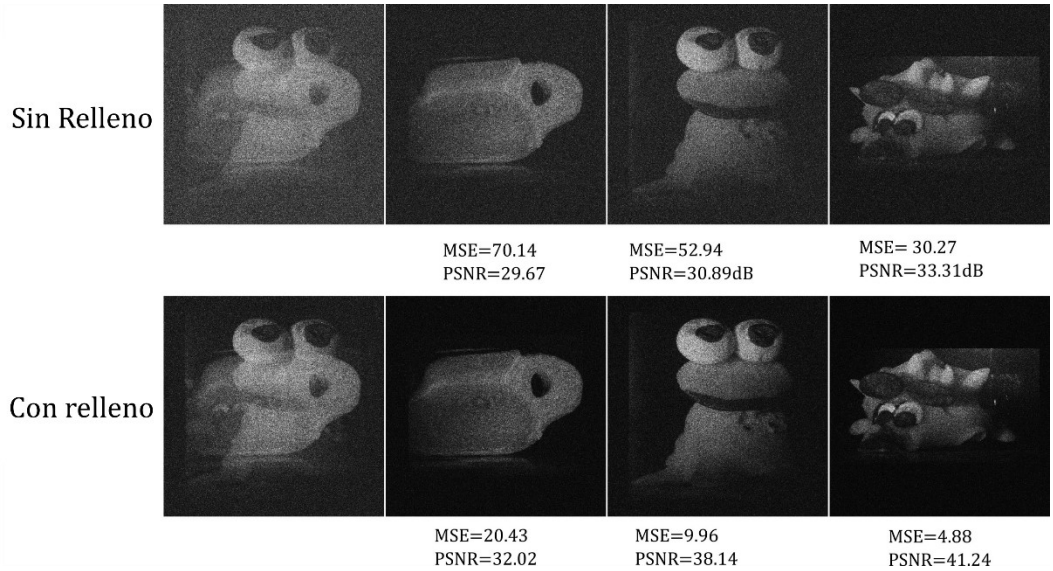

Figura 75: Objetos reconstruidos a partir de un paquete de 3 campos ópticos multiplexados.

En la Figura 75 se muestra la reconstrucción del paquete de tres campos ópticos multiplexados, cuando no se multiplica previamente por una de las máscaras binarias y cuando se multiplica con la máscara de cada objeto. Se muestran además los resultados obtenidos con relleno, y las métricas de calidad del error cuadrático medio (MSE por las siglas en ingles de "mean square error") y del pico de la relación señal ruido (PSNR por las siglas en ingles de "peak signal to noise ratio") comparado con los objetos reconstruidos de campos ópticos sin multiplexar. El MSE está definido como

$$MSE = \frac{\sum_{p,q}^{N,M} |\, m(p,q) - m_c(p,q)\,|^2}{N \times M} \tag{3.4.3}$$

Donde $m(p,q)$ y $m_c(p,q)$ son los objetos reconstruido del campo óptico sin multiplexar y multiplexado respectivamente, (p,q) son coordenadas de pixel y N, M es el número de pixeles horizontales y verticales. El PSNR se define en base al MSE como

$$PSNR = 20\log_{10}\left(\frac{2^{B-1}}{\sqrt{MSE}}\right) \tag{3.4.4}$$

Donde B es la profundidad de bit de las imágenes a comparar. El PSNR es una de las métricas más usadas para evaluaciones de calidad en técnicas de compresión con perdida [81]. En general, un PSNR entre 30 dB y 50 dB representa una buena conservación de la calidad visual. Por debajo de 30 dB, la degradación de la imagen respecto a la referencia empieza a ser notoria. En los resultados de la Figura 75 vemos

que al usar relleno todos los objetos reconstruidos están dentro del rango de PSNR aceptable, mientras que sin relleno los objetos están en la cota inferior de este rango, con el resultado correspondiente al "jarrón" por debajo de la misma.

El factor de compresión de esta técnica, sin aplicar relleno y con igual muestreo para todos los objetos, es igual a N, donde N es el número de objetos a multiplexar. Aunque en principio es posible multiplexar cualquier cantidad de objetos, en la práctica estaremos limitados por la pérdida aceptable para cada aplicación.

Además de permitir compresión, el multiplexado con máscaras binarias tiene utilidad en áreas de seguridad óptica y validación de datos, ya que para poder recuperar uno de los objetos deseados sin ruido por superposición es necesario conocer la máscara binaria con la que fue muestreado.

Las técnicas aquí mostradas demuestran la potencialidad de las técnicas opto-digitales. Adicionalmente, vale la pena señalar, que varias de ellas pueden combinarse para lograr factores de compresión aun mayores, por ejemplo, aplicando escalado óptico y disminuyendo la profundidad de bit a la vez que se descarta la información de amplitud. Realizando estas combinaciones, es posible lograr factores de compresión cercanos a los usados en compresión digital de imágenes.

IV. Visualización de datos holográficos

4.1. Introducción

En todos los trabajos presentados hasta ahora, hemos mostrado técnicas opto-digitales, en las cuales los datos holográficos correspondientes a campos ópticos son registrados experimentalmente y reconstruidos por medios digitales. Por otro lado, existe una rama de la holografía que se encarga de estudiar el proceso contrario, es decir, la generación digital de información holográfica para su posterior reconstrucción óptica. Esta área es denominada holografía generada por computador. En 1966, Brown & Lohman demostraron la síntesis de un holograma binario por computadora, y la posterior reconstrucción del mismo tras imprimirlo como una máscara binaria [82].

Este avance, en teoría, hacia posible la construcción de sistemas de visualización 3D basados en los principios de la holografía, pero la generación de hologramas digitales es costosa computacionalmente, incluso con equipos modernos, y la presencia de ruido coherente en los objetos reconstruidos es un problema difícil de solucionar [83–85].

La otra dificultad radica en la necesidad de convertir los hologramas generados por la computadora en un elemento físico que interactúe con el campo para producir la reconstrucción de los objetos deseados. En muchos de los casos, este propósito se lograba imprimiendo una máscara de transmisión binaria o iluminando punto por punto una película fotográfica. Este proceso es lento, haciendo difícil la reconstrucción de múltiples objetos de manera efectiva.

Debido a estos retos, ha existido un gran interés en sistemas electrónicos programables que permitan la proyección rápida de diagramas holográficos [86,87]. Ya que la información holográfica contiene fase y amplitud, y dado que no existen elementos

capaces de modular ambas características del campo óptico simultáneamente, las tecnologías de proyección holográfica se han dividido en aquellas basadas en la modulación de amplitud y en las de modulación de fase.

Los moduladores de amplitud fueron los primeros en ser implementados exitosamente, aunque, como mencionamos en la sección 1.8, ya que gran parte de la información de una señal está contenida en la fase, la proyección de hologramas con estos requiere de estrategias, como la introducción de imágenes gemelas, para codificar la información compleja en un diagrama de amplitud [88].

Por otro lado, los moduladores de sólo fase apenas recientemente han adquirido un desempeño que los hace viables para su uso como sistemas de proyección holográfica. En particular, los denominados moduladores espaciales de luz cristal líquido en silicio (LCoS-SLM de la siglas en ingles de "liquid crystal on silicon spatial light modulator") ofrecen altas resoluciones, pequeños tamaño de pixel y buena modulación de fase [89]. En este capítulo mostraremos una de las técnicas más comunes para codificar la información de objetos de amplitud en una fase que pueda ser proyectada y reconstruida con un LCoS-SLM. Además, mostraremos una técnica novedosa basada en el uso de máscaras de fase optimizadas, y presentaremos cómo se pueden reconstruir objetos a color a partir de fases comprimidas.

4.2. Visualización de hologramas digitales

En esta sección, nos dedicaremos a discutir la visualización de hologramas de Fourier usando SLMs de reflexión. Estos moduladores están compuestos de una capa antirreflectante, una capa de cristal líquido, una capa reflectiva (usualmente de espejos de aluminio) y finalmente un sustrato de silicio en el cual están los controles electrónicos. La capa de cristal liquida está dividida en celdas, las cuales cumplen el papel de pixeles. Dependiendo del voltaje aplicado a las celdas, se introducirá una alteración en la distribución de las moléculas de cristal líquido, lo que debido a la birrefringencia de las mismas introduce un cambio en el estado de polarización de la luz. Con el uso de polarizadores adecuados, se convierte este cambio de estado de polarización en un retardo de fase.

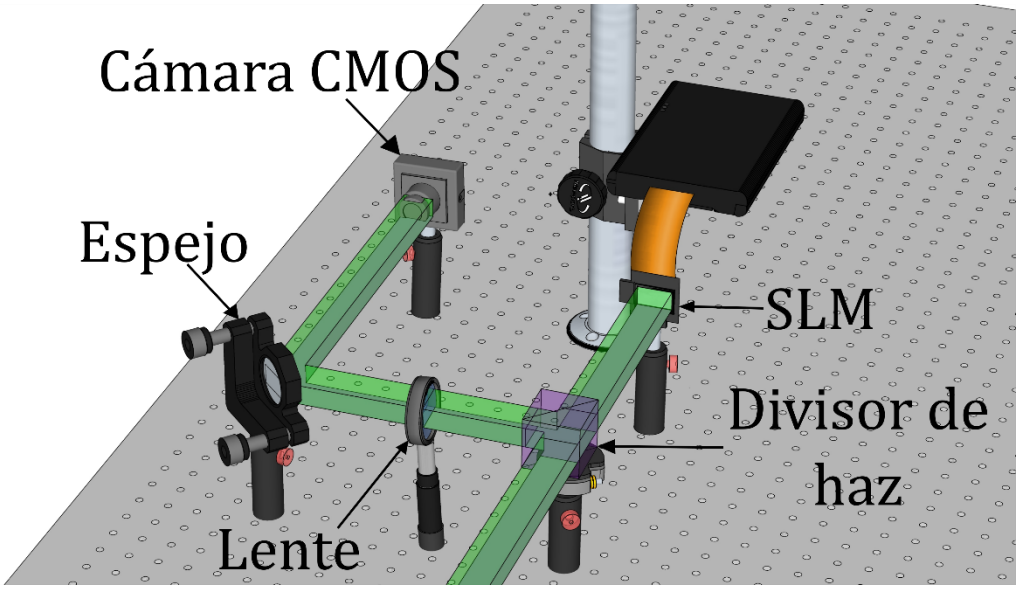

Figura 76: Esquema de un sistema para la reconstrucción de hologramas de Fourier usando un modulador espacial de luz (SLM) por reflexión.

En la Figura 76 mostramos el esquema básico para la reconstrucción de hologramas de Fourier usando un SLM por reflexión. El SLM es iluminado por una onda plana, tras lo cual adquiere la fase proyectada, y se refleja, pasando por un divisor de haz que lo dirige hacia una lente que conjuga el plano del modulador con el plano de la cámara CMOS donde se registra el objeto reconstruido.

La proyección de hologramas en moduladores de sólo fase está sometida a las mismas restricciones de resolución y tamaño de pixel que el registro de hologramas digitales, además de presentar algunas dificultades adicionales. La primera dificultad tiene que ver con la diferencia entre el número de pixeles usados para el registro del holograma original y los del SLM.

Los hologramas y objetos encriptados que hemos mostrado a lo largo de esta tesis fueron registrados con una cámara EO-10012C, con una resolución de 3840x2748 pixeles. El modulador espacial de luz de fase que empleamos en los ejemplos de esta sección es un Holoeye Pluto-SLM, con una resolución de 1920x1080.

Así pues, nuestro modulador no es capaz de proyectar directamente la información correspondiente al holograma registrado. Para solucionar este problema, podemos llevar a cabo un proceso de filtrado modificado, en el cual realizamos la TF del holograma, digitalmente recortamos el orden correspondiente al objeto, y lo rellenamos con ceros hasta que tenga el mismo número de pixeles verticales y horizontales que el modulador.

Tras aplicar la TFI a la matriz resultante, descartamos la información de amplitud, quedando la fase correspondiente al campo óptico.

La segunda dificultad es que podrán reconstruirse adecuadamente objetos cuyas TF tengan una amplitud con poca variación, tal y como discutimos en la sección 1.8. En este sentido, la proyección tendrá un mínimo de degradación debido a la perdida de la información de amplitud cuando corresponda a la fase de un objeto difuso.

El otro problema que afecta la reconstrucción es que los moduladores no tienen una eficiencia del 100%, por lo que no toda la luz que reciben será modulada. Debido a esto, el campo óptico inmediatamente después del modulador será una superposición del campo correspondiente a la fase proyectada más una onda plana sin modular. Esta onda sin modular produce un orden central intenso en el plano de reconstrucción, el cual puede superponerse con el objeto reconstruido y afectar seriamente su calidad. Para evitar este efecto, podemos multiplicar la fase a proyectar por una red de fase, cuya frecuencia sea escogida de manera que el objeto sea reconstruido lo suficientemente lejos del orden central para evitar cualquier superposición [90].

El modulador PLUTO es controlado como una pantalla adicional con una profundidad de 8 bits, por lo que la información de fase, que tiene el rango entre $-\pi,\pi$, debe ser convertida en una intensidad con valores entre 0 y 255. Realizando este proceso, obtenemos finalmente una imagen correspondiente a la información de fase, con la resolución adecuada para ser proyectada en el modulador.

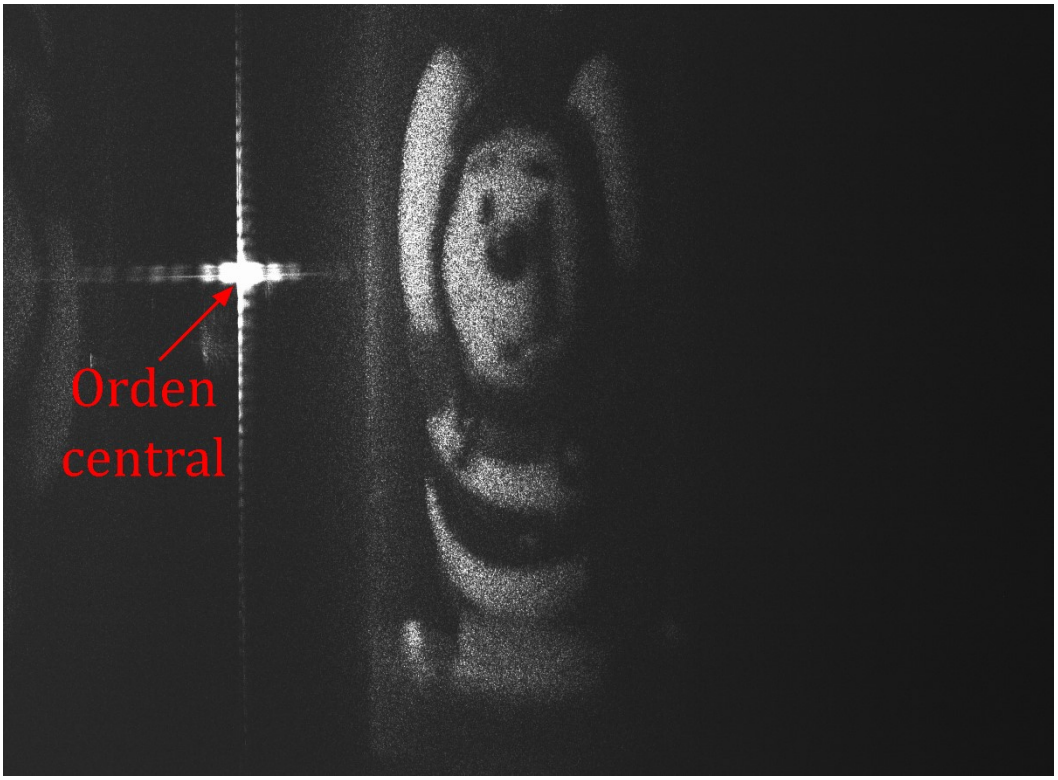

Figura 77: Objeto reconstruido con un modulador de fase pura.

En la Figura 77 se muestra el resultado de reconstruir un objeto cuyo campo óptico fue registrado con un sistema de holografía digital de Fourier, usando un modulador espacial de fase pura. Como se puede apreciar, el objeto es reconstruido adecuadamente, y gracias a la red de fase aparece a una distancia del orden central. No obstante, debido al efecto causado por el tamaño finito de los pixeles del modulador, las secciones del objeto más cercanas al orden central presentan mayor intensidad que las más lejanas. Este efecto lo encontramos en la sección 2.8, cuando discutimos la reducción de ruido de objetos encriptados, y puede mitigarse dividiendo la TF de la fase que será proyectada por una ventana de Hamming, siempre y cuando el objeto reconstruido se encuentre en el lóbulo central de difracción del SLM.

Las operaciones realizadas para poder proyectar el campo óptico imponen nuevas restricciones sobre el tamaño del objeto. En particular, que el área filtrada del holograma de Fourier debe ser menor que el área del modulador. En caso contrario, puede usarse la técnica de escalado óptico para garantizar que se cumpla esta condición.

En el caso de hologramas de Fresnel, el proceso necesario para proyectar el campo óptico es el mismo, usando el mismo esquema de la Figura 76, con la única modificación de retirar la lente. La principal precaución que se debe tomar en este caso es que al

realizar la TF del holograma de Fresnel, un orden corresponde al campo óptico de la imagen real del objeto con plano de reconstrucción a una distancia z del holograma y el otro a una imagen virtual, con plano de reconstrucción a la distancia -z. Así, debe seleccionarse el campo correspondiente a la imagen real, pues la transformada de Fresnel inversa no se puede realizar con una propagación en el espacio libre.

Al tener en cuenta esta precaución, y ubicar la cámara a una distancia z del modulador, se puede reconstruir satisfactoriamente el objeto.

Otra técnica de gran utilidad para la visualización de información con moduladores de fase consiste en multiplicar la fase del campo óptico a reconstruir con la fase de una lente. Como describimos en la sección 1.6, esto permite cambiar la posición del plano de reconstrucción de d a $\left(\frac{1}{d}+\frac{1}{f}\right)$, donde f es la distancia focal de la lente. La fase discretizada de una lente es dada por.

$$L(k,l)=\exp\left[i\frac{\pi}{\lambda f}(k^2\Delta x^2+l^2\Delta y^2)\right] \qquad (4.2.1)$$

De la ecuación anterior podemos ver que la variación de la fase se hará más rápida conforme menor sea la distancia focal de la lente, así, el tamaño de pixel del modulador limita el valor mínimo de la distancia focal de la lente virtual para poder ser muestreada adecuadamente.

Realizando esta operación, también es posible la visualización de objetos cuyos campos ópticos fueron registrados como hologramas de Fourier sin necesidad de usar lentes en el esquema experimental.

4.3. Hologramas generados por computadora.

Como vimos en la sección anterior, la visualización de objetos difusos registrados por medio de hologramas de Fresnel y Fourier puede lograrse fácilmente si se tienen los recaudos adecuados durante el filtrado. Por otro lado, si queremos visualizar información con un sistema holográfico, la generación computacional de hologramas es de mucho mayor interés, por varios motivos.

En primer lugar, se evita la necesidad de un sistema de registro de hologramas, con las complejidades que ello acarrea, las cuales hemos discutido a lo largo de esta tesis. Por

otro lado, es posible generar computacionalmente hologramas de objetos que no existen físicamente, como modelos 3D, imágenes y videos. La posibilidad de construir un objeto computacionalmente, generar su holograma y visualizarlo con un sistema holográfico que manipula el campo óptico, tal y como si se tratara de un objeto físico, tiene una gran utilidad en muchas áreas de estudio.

Es por eso que no es sorprendente que la generación de hologramas por computadora es investigada exhaustivamente, con innumerables técnicas y métodos demostrados según la aplicación, el tipo de objeto cuyo holograma se desea generar, el poder de computo disponible, y muchas otras variables.

Una de las técnicas más sencillas de generación computacional de hologramas de sólo fase está basada en la exposición que hicimos en la sección 1.8 sobre la importancia de la fase para reconstruir un objeto. Como mostramos en esa sección, si multiplicamos una imagen o un objeto por una máscara de fase aleatoria, podemos descartar la amplitud de la TF del producto resultante y reconstruir de manera aproximada el objeto original a partir de la fase. Esta fase es el holograma del objeto, y puede ser proyectada en un sistema como el de la Figura 78. Esta técnica resulta en una aproximación del objeto, con la presencia de un elevado nivel de ruido, por lo cual no es de gran utilidad en muchas aplicaciones, sin embargo, permite la generación de hologramas rápidamente y sin necesidad de procesos iterativos.

Para lograr reconstrucciones más fieles a nuestro objetivo que el método de máscara aleatoria que acabamos de describir, se puede usar el algoritmo de Gerchberg-Saxton [38]. Esta técnica ya la introdujimos brevemente en la sección 2.6.2, donde es usada para encontrar la fase de la llave en los ataques de texto plano conocido.

En general el algoritmo G-S puede usarse para hallar la fase que conecta cualesquiera dos imágenes 2D en planos conjugados. Esta característica es útil para generar hologramas de solo fase, ya que, en un sistema de visualización, como el de la Figura 76, tenemos una distribución de amplitud conocida en el plano del SLM y necesitamos hallar una fase para proyectar tal que se obtenga la amplitud deseada en el plano de reconstrucción.

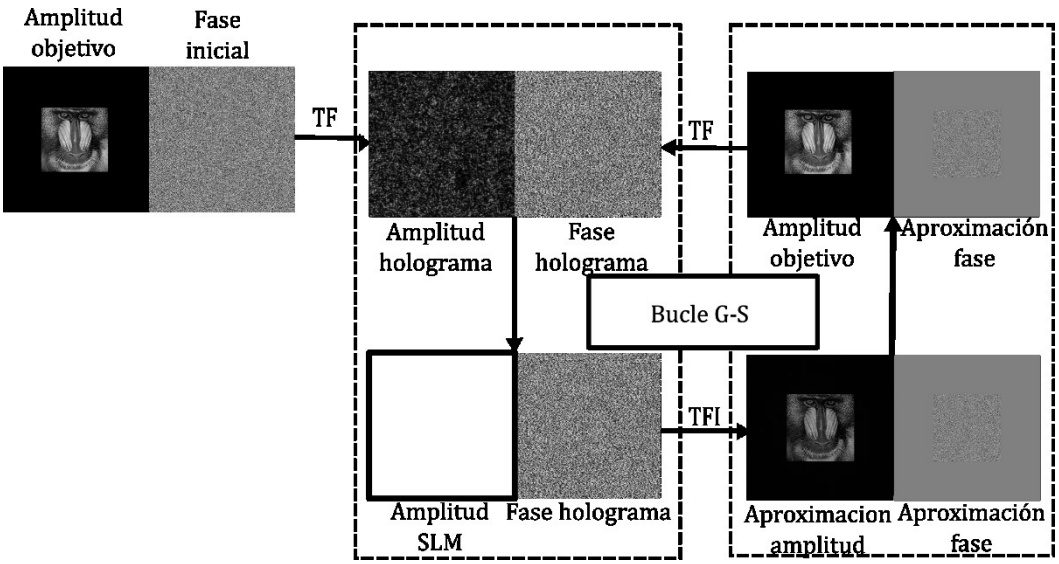

Figura 78: Esquema del algoritmo de G-S aplicado a la generación de hologramas de sólo fase.

En la Figura 78 se muestra el esquema del algoritmo de G-S. Para generar un holograma de sólo fase, primero se multiplica la amplitud objetivo por una fase inicial, la cual puede ser de cualquier forma. Luego se realiza la TF del producto, y se hace constante la amplitud de la transformada resultante. Se aplica entonces la TFI a la fase obtenida en el paso anterior, logrando así una función cuya amplitud será una aproximación a la amplitud del objetivo. Conservando la fase de esta función, se reemplaza la amplitud aproximada por la amplitud del objetivo, y se realiza la TF, completando así una iteración del algoritmo.

En cada iteración, la amplitud aproximada será más cercana a la amplitud del objetivo, y se itera hasta que se supere un valor límite de alguna métrica de comparación, como el NMSE o el coeficiente de correlación entre el objetivo y la aproximación. Esta técnica puede producir reconstrucciones con un elevado nivel de calidad, pero es un proceso iterativo relativamente lento, especialmente si se desea producir hologramas extensos o correspondientes a gran cantidad de objetos.

En la búsqueda de un método para la generación de grandes cantidades de hologramas rápidamente, para aplicaciones de visualización de información dinámica, en Velez *et al* [91] propusimos una técnica que combina la velocidad de la generación de hologramas del método de fase aleatoria con la calidad de reconstrucción superior que se puede lograr con el algoritmo G-S.

La propuesta consiste en usar el algoritmo de G-S para optimizar una máscara de fase aleatoria para los parámetros del sistema de reconstrucción, como lo son la resolución, el

tamaño de pixel, la longitud de onda y el tamaño de los objetos a ser reconstruidos. Luego, se usa esta fase aleatoria optimizada (ORAP por las siglas en ingles de "Optimized random phase") para generar los hologramas de fase, multiplicando los objetivos con esta ORAP, realizando la TF del producto y descartando la amplitud.

Para generar la ORAP, multiplicamos una ventana, la cual es una función rect del mismo tamaño y resolución de los objetivos cuyos hologramas deseemos generar, por una máscara de fase aleatoria inicial. Posteriormente, realizamos la TF del producto, y aplicamos varias iteraciones del algoritmo de G-S, en cada una usando esta ventana como objetivo. Una vez la reconstrucción de la ventana se aproxima lo suficiente a la ventana original, extraemos la fase de la reconstrucción. Esta fase corresponde a la ORAP con la cual podemos generar cualquier número de hologramas, multiplicando los objetivos con esta ORAP, realizando la TF del producto y descartando la amplitud. En la Figura 79 se muestra el esquema de la técnica propuesta.

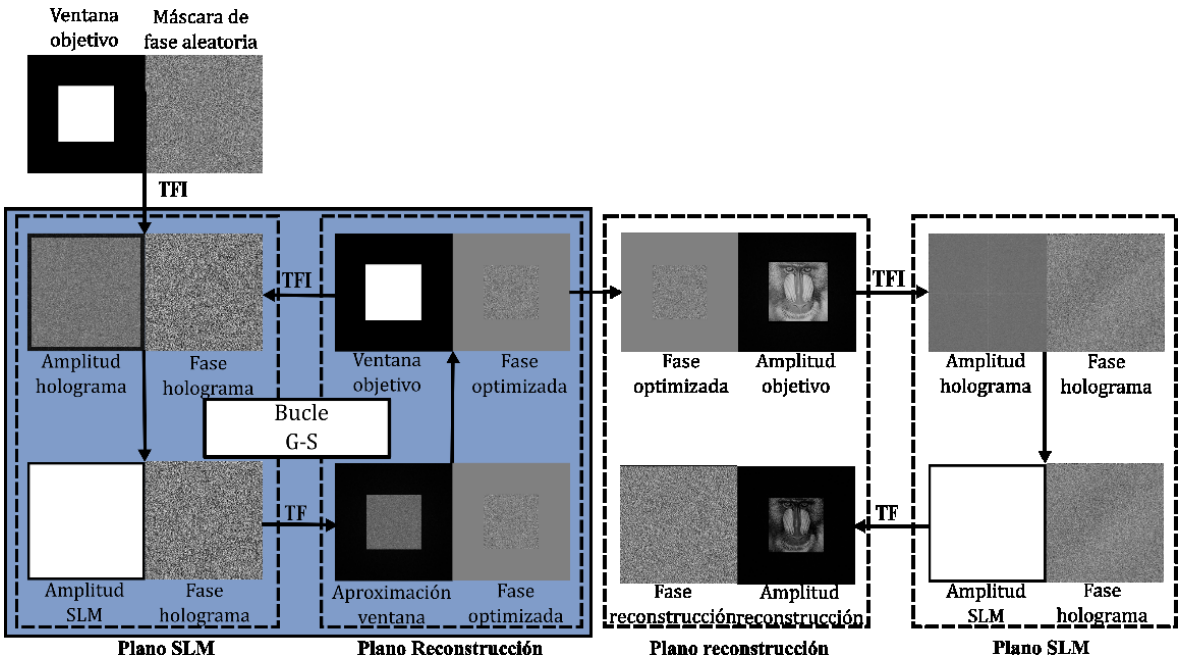

Figura 79: Esquema de la técnica de generación de hologramas de sólo fase con ORAP.

El proceso de optimización de la máscara de fase, tiene como propósito hacer que se cumplan las condiciones de reconstrucción a partir de la fase de una señal, tal y como se discutió en la sección 1.8. En particular, garantiza que la TF de la ORAP tenga el mínimo de variación posible en su amplitud, reduciendo así la perdida de información al hacer la amplitud constante. Adicionalmente, con esta técnica logramos que el ancho de banda de la máscara optimizada sea lo más parecido posible a la del sistema de proyección. La

ORAP sólo debe ser generada una vez para un sistema óptico dado, y sólo debe regenerarse si este sufre alteración de alguno de sus parámetros, como la resolución, tamaño de pixel, tamaño de los objetos o longitud de onda, haciendo así innecesario el uso de procesos iterativos cada vez que se desea generar un nuevo holograma.

A continuación, determinaremos, a través de una simulación, la dependencia del coeficiente de correlación entre el objeto original y el objeto reconstruido a partir de hologramas de fase generados con el método de ORAP, en función del número de iteraciones del algoritmo G-S usadas para optimizar la máscara de fase. La resolución del SLM usado en la simulación fue de 1080x1080 pixeles con tamaño de píxel de 8 $\mu m \times$ 8 μm. La ventana objetivo y el objeto cuyo holograma se desea generar, tiene un tamaño de 1000x1000 pixeles. La transformada de Fourier es realizada por una lente convergente con 200mm de distancia focal. Finalmente, la longitud de onda de la iluminación usada en la simulación es de 532nm

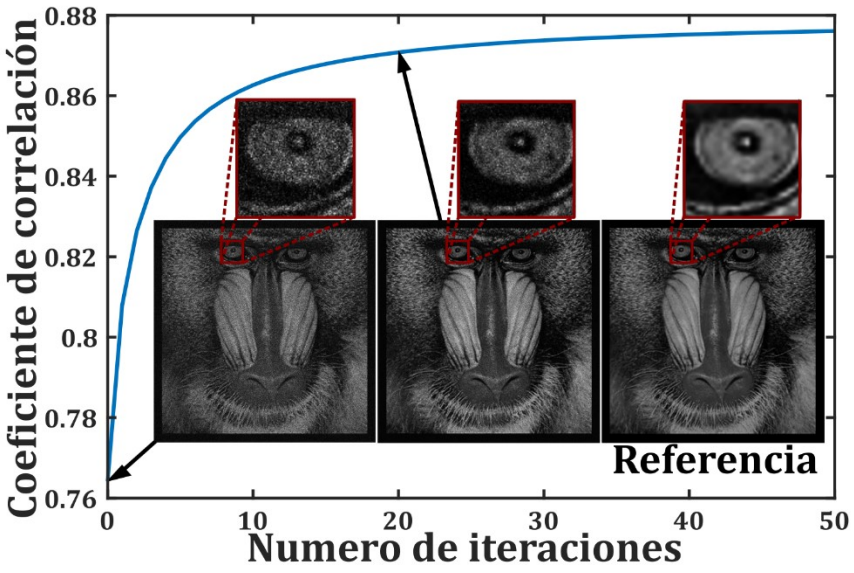

Figura 80: Coeficiente de correlación entre el objeto reconstruido a partir de hologramas generados con ORAPs el objeto original (Referencia) en función del número de iteraciones del algoritmo G-S.

En la Figura 80 podemos apreciar como la calidad de reconstrucción, evaluada con el coeficiente de correlación, inicialmente se incrementa rápidamente conforme se aplican más iteraciones en el proceso de optimización de la fase aleatoria, pero cada iteración subsecuente produce un menor aumento en el coeficiente de correlación. Las imágenes incrustadas en la curva respaldan la efectividad del proceso de optimización,

presentando mayor ruido de speckle cuando no se optimiza la fase (correspondiente a 0 iteraciones en la máscara) que después de emplear 20 iteraciones.

Teniendo en cuenta este resultado, ahora procederemos a comparar la técnica de generación de hologramas con ORAP con el uso de fases no optimizadas y la aplicación directa del algoritmo G-S a la generación del mismo objeto usando las tres técnicas expuestas hasta ahora. Luego calcularemos el coeficiente de correlación y el PSNR entre los objetos reconstruidos y el objeto original. Para esta prueba se usaron 20 iteraciones del algoritmo G-S, tanto para la optimización de la fase aleatoria como para la aplicación directa.

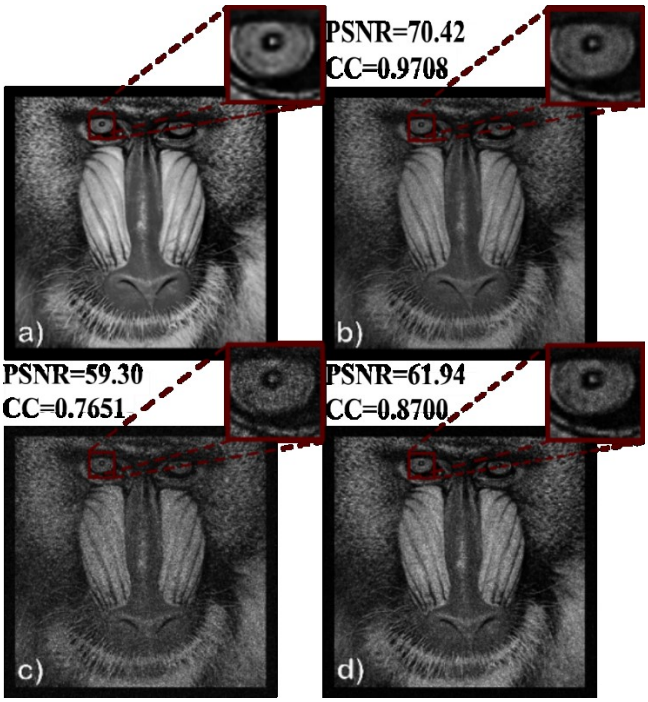

Figura 81: a) objeto original, b) objeto reconstruido a partir de un holograma resultante de aplicar directamente el algoritmo G-S, c) objeto reconstruido a partir de un holograma generado con una fase aleatoria sin optimizar, d) objeto reconstruido a partir de un holograma generado con una fase aleatoria optimizada.

Los resultados de la Figura 81 muestran como la aplicación directa del algoritmo de G-S produce un holograma con la mejor calidad de reconstrucción entre los tres métodos que estamos comparando (Figura 81.b). Los hologramas generados con máscaras aleatorias sin optimizar producen la reconstrucción más deficiente (Figura 81.c). Los resultados con ORAP (Figura 81.d) ofrecen una calidad de reconstrucción significativamente superior a las fases aleatorias sin optimizar, y a la vez manteniendo las ventajas de esta técnica en cuanto a velocidad de computo se refiere.

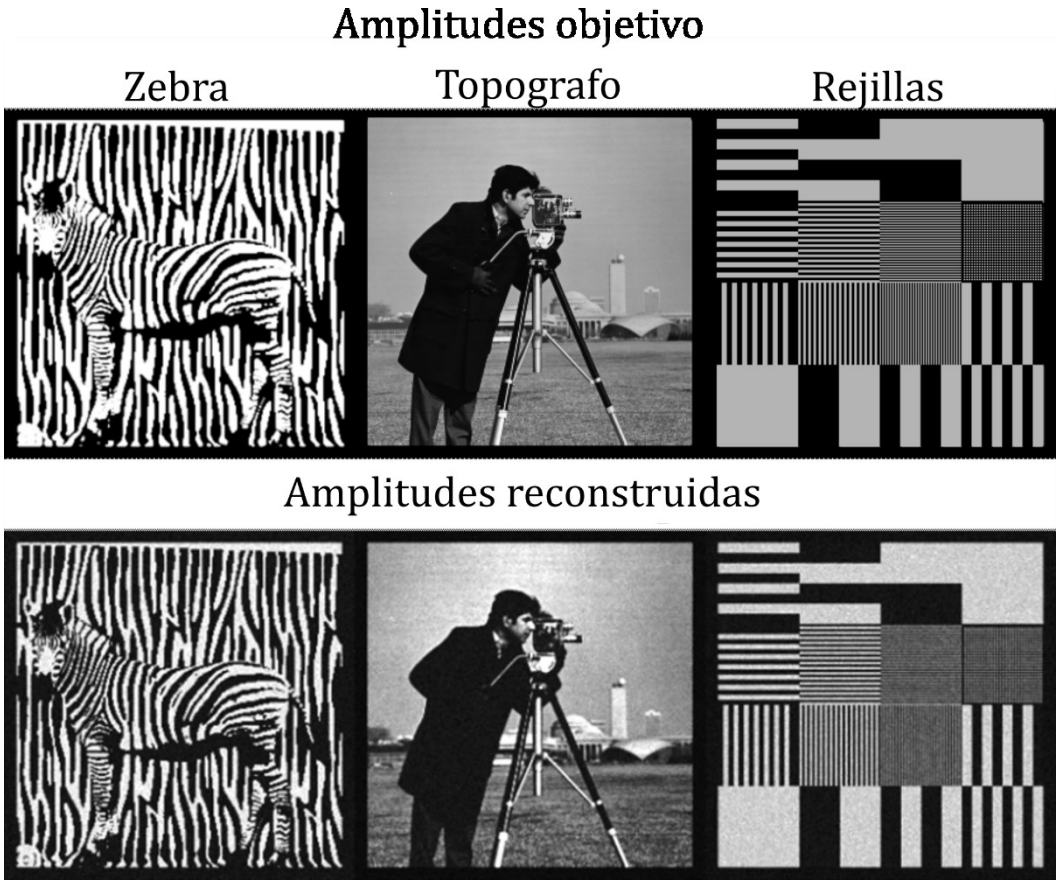

Figura 82: Reconstrucción de diferentes objetos a partir de hologramas generados con la misma ORAP.

En la Figura 82, mostramos como la misma ORAP generada para obtener el resultado de la Figura 81 se puede usar para obtener hologramas de solo fase de otros objetos, sin necesidad de repetir el proceso de optimización. Como se puede apreciar, la calidad de la reconstrucción no varía fuertemente al usar distintos tipos de objeto. Para verificar esta observación de forma cuantitativa, procedemos a repetir la prueba de la Figura 80 para los objetos presentados en la Figura 82

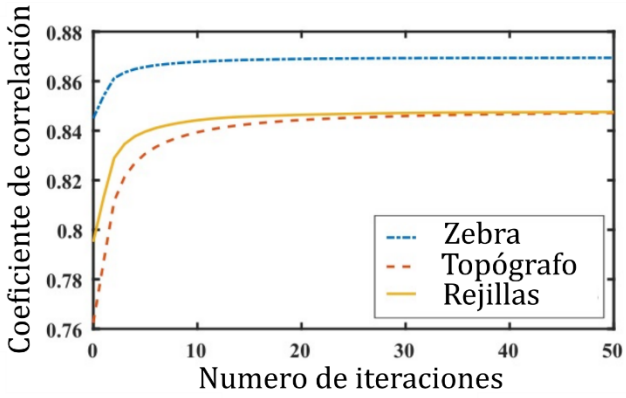

Figura 83: Coeficiente de correlación entre los objetos reconstruidos a partir de hologramas generados con ORAPs y los objetos originales en función del número de iteraciones de G-S.

Los resultados de la Figura 83 confirman que el comportamiento de las ORAP no varía significativamente con el objeto. En particular, los objetos binarios con pocas frecuencias espaciales, como la Zebra, muestran un coeficiente de correlación ligeramente superior.

En la Tabla 3 se muestra el tiempo de cómputo necesario para generar los hologramas de los objetos usados en la Figura 81 y Figura 82. La generación de los cuatro hologramas de sólo fase aplicando directamente el algoritmo de G-S tomo 2.384 segundos. Para generar los hologramas de los mismos objetos por medio de ORAPs, se requirieron 0.745 segundos, sin embargo, de ese tiempo, 0.521 segundos corresponden a la optimización de la máscara de fase. Una vez obtenida esta máscara, cada holograma se puede generar en 0.056 segundos, comparado con los 0.596 segundos requeridos con la aplicación directa del algoritmo de G-S. Estos resultados hacen evidente las ventajas en velocidad de computo que ofrece la generación de hologramas con ORAPs. Para todos los resultados numéricos presentados en esta sección, se usó una computadora equipada con una CPU Ryzen 7 1700 y una GPU NVIDIA GTX 1060. Todos los programas fueron escritos en MATLAB empleando procesamiento en GPU.

Tabla 3: Tiempo de cómputo usado para la generación de hologramas de fase con una ORAP y aplicando el algoritmo de G-S directamente a los objetos.

Proceso	**ORAP (*s*)**	**G-S (*s*)**
Generación ORAP	0.521	–
Holograma Mandril	0.056	0.596
Holograma Zebra	0.056	0.596
Holograma Topógrafo	0.056	0.596
Holograma Rejillas	0.056	0.596
Tiempo total	0.745	2.384

Una vez realizados los análisis numéricos para determinar el desempeño de los métodos explicados en esta sección, procedemos a confirmar experimentalmente la reconstrucción de los hologramas generados con un sistema de visualización de datos holográficos. Para este propósito usamos el sistema de la Figura 76. Se generaron hologramas de 1080x1080 pixeles, usando los mismos parámetros del montaje experimental, que en este caso consisten en una longitud de onda de 532nm, tamaño de pixel de $8\,\mu m \times 8\,\mu m$ y una lente convergente de 150mm de distancia focal.

Aquí vale la pena resaltar que, aunque el SLM que usamos para modular la fase tiene una resolución de 1920x1080 pixeles, sólo usamos de estos 1080x1080 pixeles para la fase de los hologramas generados. Esto es para evitar la distorsión de los objetos reconstruidos debido a la presencia de un número mayor de pixeles en la dirección horizontal que en la vertical del modulador. Esta distorsión hace que, en el plano de reconstrucción usado durante la generación computacional del holograma, el tamaño de pixel en la dirección horizontal sea diferente a la vertical. Como resultado, al realizar la reconstrucción óptica, se produce un estiramiento del objeto en la dirección contraria al eje con mayor número de pixeles en el modulador.

Aunque este efecto puede corregirse aplicando un estiramiento en la dirección contraria al objeto antes de generar su holograma, en estos resultados se resolvió el problema haciendo los hologramas cuadrados, y asignando a la fase de los pixeles restantes del modulador un valor constante. La luz que incide en estos pixeles resultará en un aumento de la intensidad del orden central en el plano de reconstrucción, pero no afectará de otra forma la calidad del objeto recuperado.

Como se explicó en la sección anterior, se proyecta en el SLM el producto entre los hologramas generados y una red de fase, evitando asi la superposición entre la reconstrucción y el orden central.

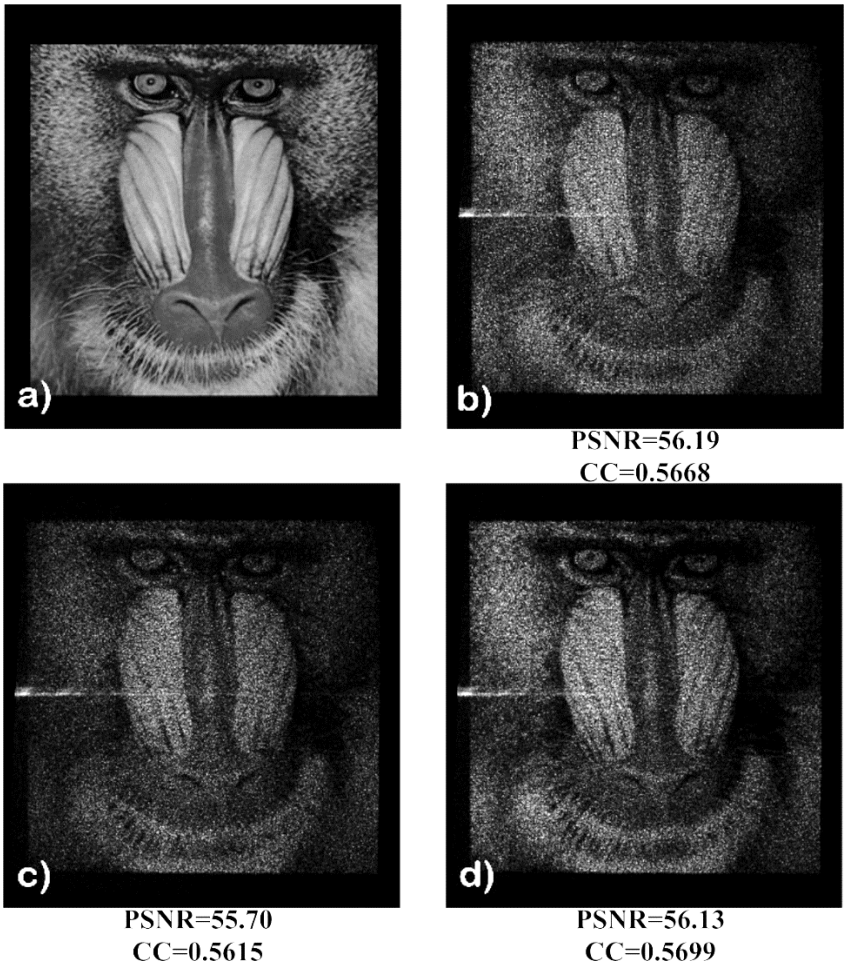

Figura 84: Reconstrucción óptica de un objeto a partir de hologramas generados por computadora. a) objeto original, b) reconstrucción del holograma generado con aplicación directa de G-S, c) reconstrucción del holograma generado con fase aleatoria sin optimizar, y d) reconstrucción del holograma generado con ORAP.

Las reconstrucciones experimentales de la Figura 84 tienen un comportamiento similar al de las reconstrucciones numéricas, y aunque los tres métodos presentan valores similares tanto del PSNR como del coeficiente de correlación, el método de G-S directo y el de ORAP muestran una mejor reconstrucción que el de fase no optimizada. Este resultado permite concluir que, para la visualización experimental, el método de ORAP presenta una calidad de reconstrucción muy similar al del G-S, a la vez que mantiene significativas ventajas en términos de la velocidad de generación de hologramas.

Los resultados experimentales aquí mostrados presentan un nivel de ruido superior al de los resultados numéricos. El motivo de este ruido es la presencia de fases aleatorias en el plano de reconstrucción, efecto que también está presente en la recuperación de objetos difusos a partir de hologramas digitales. Una forma de reducir este ruido consiste

en proyectar en forma sucesiva hologramas del mismo objeto generados usando distintas fases al inicializar el algoritmo de G-S. La reconstrucción de cada holograma presentará un diferente ruido, y al promediarse temporalmente se obtiene una reducción en el efecto del mismo [59].

Esta técnica, aunque simple, hace mucho más lenta la visualización de hologramas, ya que para una reducción notable del ruido se requieren entre 5 y 10 hologramas por objeto. Aplicando directamente el algoritmo G-S, y teniendo en cuenta los resultados aquí expuestos, se necesitarían entre 11 segundos y 23 segundos para generar las fases correspondientes. Claramente, con esta técnica no son posibles aplicaciones en tiempo real. Por ejemplo, un proyector de video tiene frecuencias de refresco de entre 30 y 60 Hz, correspondientes a una duración por cuadro de entre 0.033 y 0.016 segundos. Este es el tiempo máximo que puede tardar la generación del holograma si se desea usarlos en este tipo de aplicaciones. Como podemos ver, la generación de un solo holograma con ORAP, que toma 0.0267 segundos, está justo en este intervalo temporal, pero continúa siendo insuficiente para poder aplicar reducción de ruido con promediado temporal. Aun así, la técnica ORAP ofrece la posibilidad de controlar el campo óptico en tiempo real.

4.4. Visualización de hologramas a color

La visualización de hologramas a color requiere de un aumento de la complejidad del sistema de reconstrucción, razón por la cual la mayoría de los trabajos en el área se han centrado en datos monocromáticos o de una sola longitud de onda. Como expusimos en la sección 1.7, el registro de hologramas a color requiere de múltiples fuentes de iluminación, las cuales determinaran el espacio de color de los objetos reconstruidos. En el caso de la visualización, este requisito es el mismo, es decir, nuestro sistema necesita un numero de longitudes de onda que determinan el espacio de color que se puede proyectar adecuadamente.

En el caso de tres longitudes de onda, es necesario modular con la información correspondiente a los hologramas registrados en cada canal tres campos ópticos de manera independiente. La forma más directa de lograr esto es usar tres SLMs, sin embargo, combinar los tres campos modulados para que coincidan los planos de reconstrucción hace necesario de componentes ópticos adicionales, aumentando el tamaño y la complejidad del sistema.

Por otro lado, aun combinando exitosamente los haces, recordemos que las lentes convergentes presentan aberraciones cromáticas, lo que hace que, si se usa una sola lente para realizar la TF de los tres campos, se obtendrán distintos planos de reconstrucción para cada longitud de onda. En este sentido, o se transforman por separado cada campo, o se usan lentes digitales para cambiar la posición del plano de reconstrucción de cada campo por separado, tal y como se describe en la sección 4.2.

Debido a estas complicaciones, algunos trabajos han buscado alternativas para lograr la visualización de información holográfica a color usando un solo modulador. Entre las estrategias propuestas encontramos una en la que se realiza un multiplexado temporal de las distintas longitudes de onda. En esta propuesta, los hologramas correspondientes a cada longitud de onda son proyectados secuencialmente en el mismo SLM, con un sistema que alterna de manera sincronizada la iluminación sobre el mismo [92,93].

Esta proyección secuencial, si se realiza a una velocidad lo suficientemente elevada, puede resultar en una reconstrucción que visualmente parece estar a color, debido a que los ojos o cámaras tienen un tiempo de integración finito. Este método está limitado principalmente por la velocidad a la que se puede "refrescar" el modulador, es decir, cuanto tiempo toma cambiar de una fase a otra. En la mayoría de los moduladores, esta frecuencia de refresco está limitada a 60Hz, lo que es demasiado lento para el ojo humano, produciendo la percepción de una imagen intermitente.

Otra técnica consiste en realizar un multiplexado con modulación por redes de fase de los tres hologramas [94], correspondientes a cada canal. La idea detrás de este método consiste en multiplicar la fase de cada canal por una red con una frecuencia y orientación diferente, y proyectar la suma de las tres fases en el modulador, el cual es iluminado con todas las longitudes de onda simultáneamente. Las redes hacen que la reconstrucción de cada canal aparezca en un lugar del espacio diferente, con una separación espacial que permita filtrar los artefactos indeseados causados por iluminar el holograma con longitudes de onda incorrectas. Tras realizar este filtrado se puede usar un sistema óptico para combinar los objetos reconstruidos, resultando en la recuperación del objeto a color.

A diferencia del multiplexado temporal, este método no requiere de moduladores de alta frecuencia de refresco ni de sincronizar la iluminación con el SLM. Sin embargo, la necesidad de realizar el filtrado ópticamente y luego añadir elementos para combinar la reconstrucción de los distintos canales, hace a esta técnica difícil de implementar.

La última propuesta para visualizar información a color con un solo SLM es el multiplexado de división espacial. En este método, se divide el modulador en regiones, en las cuales se proyecta la fase correspondiente a un color, iluminando cada región solo con una de las longitudes de onda [95]. Este método tiene bajos requerimientos para su implementación, necesitando un mínimo de elementos ópticos adicionales en el sistema, pero tiene la desventaja de reducir la resolución efectiva del modulador para proyectar el holograma de cada canal. Esta es la técnica que decidimos implementar.

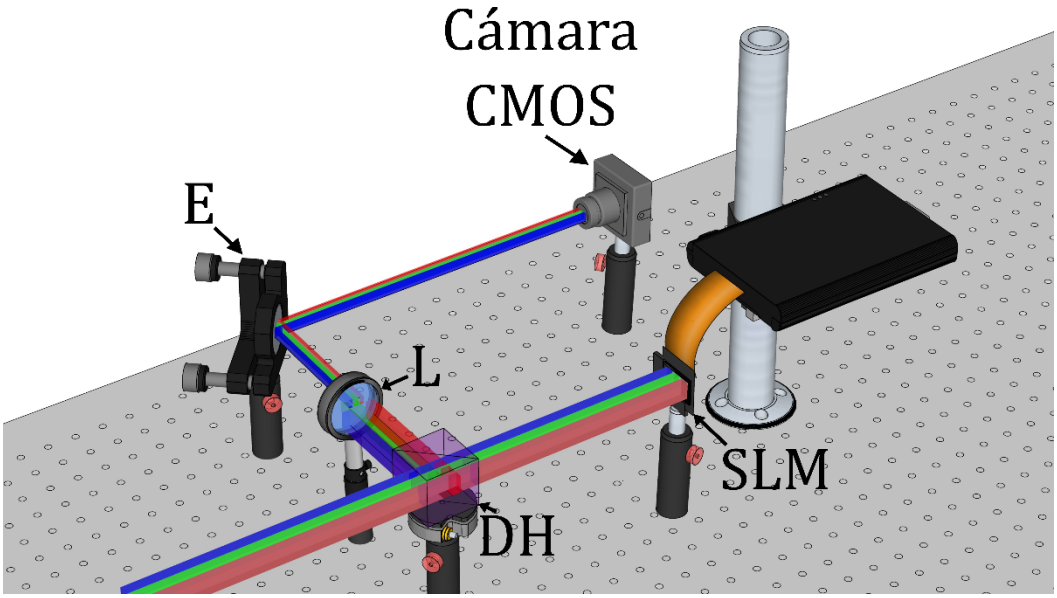

Figura 85: Sistema para la reconstrucción de hologramas de Fourier a color usando un modulador espacial de luz por reflexión. E: espejo, L: lente, DH: divisor de haz

En la Figura 85 mostramos el esquema usado para la visualización de hologramas de Fourier a color. La iluminación usada corresponde a un láser DPSS de 532 nm y 300mW de potencia, otro de 472 nm con 150 mW y finalmente un láser de helio-neón de 632.8nm y 70 mW de potencia. La lente usada en la reconstrucción es de 150 mm. El modulador es el mismo de la sección 4.2. Para registrar la intensidad de los objetos reconstruidos se usa una cámara CMOS EO-10012C de 3840x2748 pixeles con un tamaño de pixel de 1.67 $\mu m \times 1.67\ \mu m$.

Los hologramas a proyectar fueron registrados con el sistema de la sección 1.7.2. A estos se los sometió a un procesamiento consistente en los siguientes pasos.

1. Se recortaron pixeles del holograma de cada canal para evitar diferencias en las escalas de los objetos reconstruidos, tal y como se explica en la sección 1.7.3.

2. Se realizó la TF de los hologramas resultantes de 1, y se filtró el orden correspondiente al objeto, rellenando el área filtrada hasta un tamaño igual a 640x1080 pixeles, y luego se realizó la TFI.

3. Se descartó la amplitud del campo obtenido en 2, y se multiplico la fase de cada uno de los canales por una fase esférica, para compensar la aberración cromática de la lente de reconstrucción, y por una rejilla de fase para evitar los efectos del orden central. De esta manera, garantizamos que los tres canales se reconstruyan en la misma posición del espacio.

4. Se colocaron las tres fases lado a lado y se proyectan.

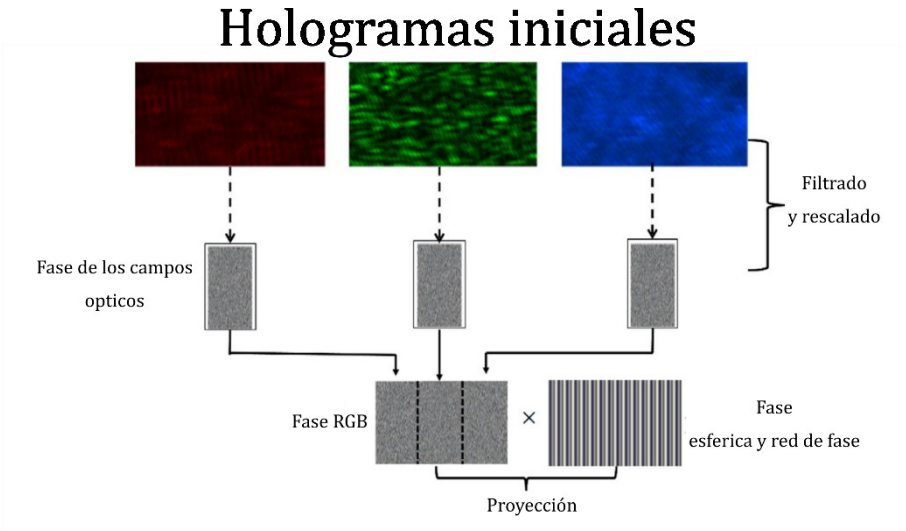

Figura 86: Esquema del procesado de hologramas digitales a color para su reconstrucción óptica.

En la Figura 86 se muestra el esquema del proceso usado para preparar los hologramas a color para su reconstrucción con un modulador de fase con multiplexado de división espacial.

Figura 87: Reconstrucción experimental de tres hologramas a color.

Como se puede apreciar en la Figura 87, el sistema propuesto es capaz de reconstruir los hologramas a color, sin embargo, el hecho de que se disponga únicamente de 640x1080 pixeles para reconstruir cada canal del objeto, limita la calidad y el tamaño de los objetos reconstruidos.

Usando este mismo sistema, en la referencia [96] demostramos por primera vez la reconstrucción óptica de datos holográficos comprimidos a color. Usando la técnica de muestreo aleatorio expuesta en la sección 3.4, multiplexamos las fases correspondientes a tres objetos a color con máscaras binarias aleatorias y ortogonales. Las fases procesadas tienen la información de los tres canales y ocupan un volumen de datos de 1.977 MB, correspondiente a un arreglo de 1920x1080 pixeles con una profundidad de 8 bits por pixel. Las máscaras aleatorias usadas tienen cada una 33% de pixeles blancos, resultando en un factor de compresión tras el multiplexado de 3. El diagrama de este proceso se muestra en la Figura 88.

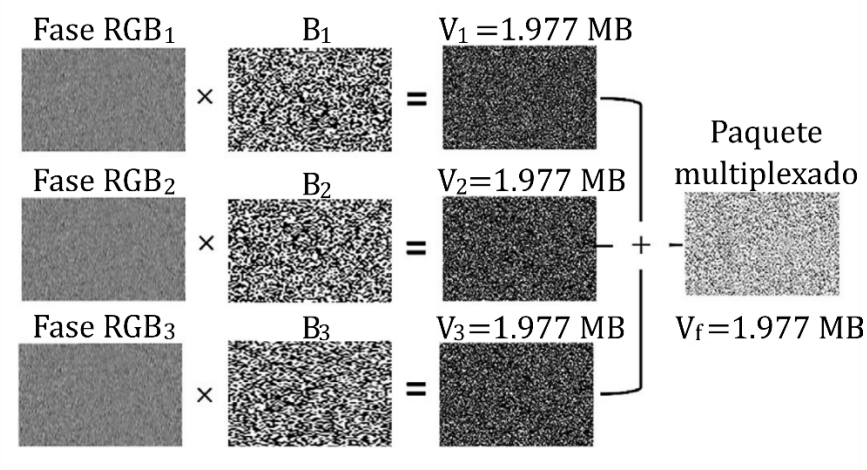

Figura 88: Esquema del muestreo de fases de objetos a color usando mascaras binarias aleatorias. B: mascara binaria, Fase RGB: fase procesada del objeto a color, V: volumen de datos.

Una vez realizado el multiplexado, procedemos a probar la reconstrucción óptica. Como se puede apreciar en la Figura 89, proyectar el paquete directamente sin antes multiplicarlo por alguna de las máscaras binarias resulta en la superposición de los tres objetos, haciendo difícil identificar la información específica de cada uno. Por otro lado, al multiplicar el paquete por una de las máscaras binarias, se obtiene el objeto correspondiente, con una degradación.

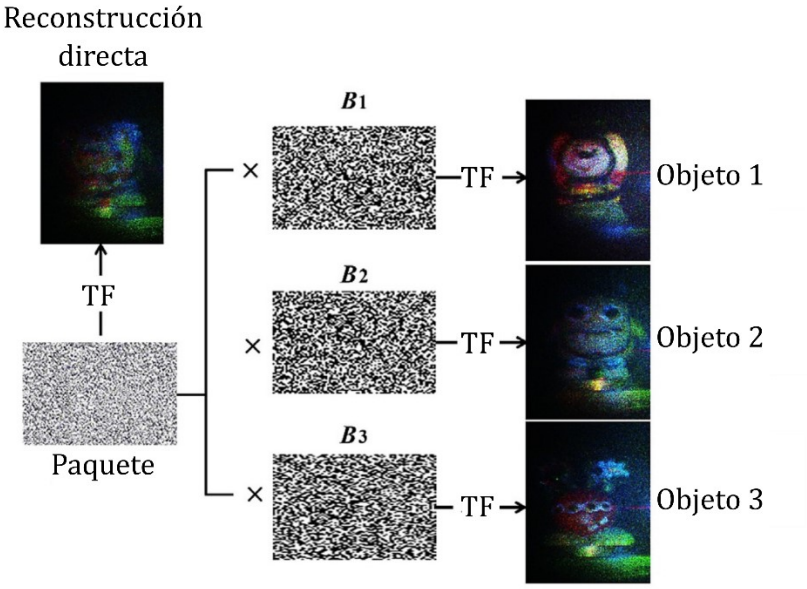

Figura 89: Reconstrucción óptica de hologramas multiplexados con máscaras binarias aleatorias.

A diferencia de lo que ocurre en la reconstrucción digital mostrada en la sección 3.4, en la recuperación óptica la degradación no se debe únicamente a la convolución aleatoria, sino que hay un ruido adicional, debido a que en un modulador de fase los

pixeles “negros” de la máscara binaria no corresponden a una amplitud cero, sino a una fase constante. Debido a este efecto, la luz que incide en los pixeles que deberían ser negros produce un aumento en la intensidad del orden central y un fondo de speckle causado por la TF del diagrama aleatorio correspondiente a los mismos. En este sentido, aunque la prueba realizada es una demostración de la posibilidad de visualizar datos holográficos a color comprimidos, el desempeño de la técnica no es ideal. Para lograr una reconstrucción más fiel a los resultados numéricos, será necesario crear versiones de amplitud de la mascará binaria, ya sea imprimiéndolas físicamente o usando un modulador de amplitud en contacto con el modulador de fase.

Usando el proceso de compresión aquí descrito, inicialmente teníamos nueve hologramas de 3840x2748 de resolución, correspondientes a un volumen de 10.06 MB para cada uno de los tres canales de cada uno de los tres objetos, para un volumen total de 90.54 MB. Tras el procesamiento de filtrado y de preparación para la visualización, obtenemos tres fases RGB de 1.977 MB, para un total de 5.931 MB. Tras el multiplexado con las máscaras binarias, este volumen se reduce a 1.977 MB. El factor de compresión final es de 45.79.

De esta manera, hemos logrado mostrar por primera vez la compresión y la reconstrucción óptica de datos holográficos con factores de compresión que se acercan a los usados por las técnicas digitales estándar en la industria para el procesamiento de imágenes y videos.

Conclusiones

Como nos planteamos en la introducción de este trabajo de tesis, hemos logrado recorrer diversos temas relacionados con la holografía digital, desde la encriptación hasta la visualización de información holográfica, estableciendo conexiones entre las técnicas usadas en cada una de las áreas exploradas.

Como ejemplo destacado, tras introducir los métodos básicos de filtrado en el primer capítulo, recurrimos a esta técnica de manera consistente en toda la extensión del presente trabajo, y luego la analizamos desde el punto de vista de la compresión.

También establecimos claramente la conexión entre la holografía digital y los sistemas de encriptación, y en el marco de este estudio proponemos soluciones a los dos problemas principales que los aquejan: Las vulnerabilidades ante ataques y la degradación de los objetos encriptados.

Respecto a las vulnerabilidades, el método de salteado expuesto presenta numerosas ventajas, ya que el simple hecho de hacer el multiplexado propuesto protege en contra de todas las categorías principales de ataques que se encuentran en la literatura. Adicionalmente, al ser este un método opto-digital, puede aplicarse a sistemas de encriptación ya existentes, sin necesidad de alteraciones en los montajes experimentales y sin añadir complejidad a los mismos. Por otro lado, introducir el salteado criptográfico al dominio de la óptica enriquece el área del criptoanálisis óptico con conceptos cuya efectividad ya ha sido ampliamente demostrada en los sistemas digitales, y abre las puertas a nuevas investigaciones sobre posibles alternativas de salteado que ofrezcan mejor desempeño.

Respecto a la degradación de los datos encriptados, realizamos tres contribuciones específicas de gran utilidad a la hora de mejorar el desempeño de los sistemas ópticos.

La primera contribución consiste en extender el concepto de contenedor de la información, los cuales fueron introducidos en la forma de códigos QR como una manera

de mitigar los negativos efectos del ruido sobre la información procesada ópticamente. Los trabajos originales donde se presentó la idea propusieron los códigos QR basándose en su ubicuidad y sus características de resistencia al daño, sin embargo, la estructura de los mismos no está directamente optimizada para los métodos ópticos. De esta manera, analizando los sistemas de encriptación ópticos, determinamos una serie de condiciones que debería reunir un contenedor especializado para ofrecer un rendimiento superior, y propusimos uno de estos contenedores: El CCOS, el cual muestra una mejora significativa en todas las métricas probadas respecto a los códigos QR cuando es usado en criptosistemas ópticos.

Como consecuencia de la efectividad de los CCOS, podemos concluir que la investigación de la holografía digital y la encriptación se beneficiarían tanto de un estudio de las limitaciones propias a las mismas, como también del estudio de las características óptimas que debe tener una información para ser registrada con la menor degradación posible, derivando así en nuevas representaciones de datos especializadas para un procesamiento óptico.

En este sentido apunta la segunda contribución que realizamos en el área de reducción de ruido de datos encriptados, en la cual retornamos al planteamiento matemático de la encriptación con doble mascara de fase para aislar una de las fuentes de ruido comúnmente despreciadas. Esta fuente es el llamado ruido de correlación aleatoria, y en base al análisis de éste, determinamos una modificación en la configuración de los datos a ser procesados, lo que resulta en una disminución significativa de la degradación debido al proceso óptico.

Esta contribución apunta a la posibilidad de implementar elementos de proyección especializados, que tomen ventaja de las características del RCN para así minimizar los efectos de este, y de esta manera ampliar el rango de aplicaciones posibles de los criptosistemas ópticos.

Como ultima contribución sobre el tema, nos volcamos al análisis general de los factores causantes de ruido en una implementación experimental del criptosistema de correlador de trasformada conjunta. En este análisis tuvimos en cuenta factores como las variaciones en amplitud de las máscaras de fase, el tamaño finito de los pixeles del medio de registro, y el ruido de correlación aleatoria, entre otros. Considerando las técnicas expuestas

anteriormente e introduciendo el concepto de máscara de referencia para corregir las variaciones de amplitud de los difusores físicos, desarrollamos un protocolo completo que reduce el ruido en un alto grado, permitiendo el procesado óptico de objetos con gran contenido espectral y escalas de grises.

Estos avances en la reducción de ruido demuestran que es posible mitigar en gran medida una de las principales desventajas de los criptosistemas ópticos. Gracias a estas mejoras, podemos prever sistemas de registro holográfico seguros, basados en DRPE. que no comprometan seriamente la calidad de la información, a la vez que se incrementa enormemente la complejidad de los contenedores y representaciones que puedan ser procesados con los mismos.

Como otra contribución en el área de la encriptación, proponemos el uso de información 3D tanto como objeto de entrada como llave de seguridad, demostrando el poder de las técnicas holográficas para procesar datos de diversa índole con éxito, inclusive sin aplicar ninguna de las técnicas ya expuestas para la reducción de ruido. Como perspectiva de esta contribución, nos planteamos la posibilidad de realizar registros dinámicos de escenas extendidas tridimensionalmente, usando otra escena dinámica extendida como llave de seguridad, obteniendo así una llave en cuatro dimensiones, cuyas características de vulnerabilidad a ataques y de generación de ruido de correlación deben ser analizadas cuidadosamente. Estas capacidades, combinadas con las metodologías de holografía a color, pueden llevar a registros seguros de escenas naturales con elevado grado de fidelidad.

En el ámbito de la compresión de datos holográficos, mostramos algunas de las estrategias más directas de compresión digital, examinando además el efecto del filtrado y de la profundidad de bit sobre el volumen almacenado. Luego, presentamos nuestras propuestas de compresión basados en sistemas ópticos. Estas técnicas representan avances interesantes, pues se constituyen en algunos de los pocos trabajos en comparar directamente el desempeño de un proceso óptico y el de uno digital en el caso específico de compresión de información holográfica, mostrando además la diferencia que existe ente el comportamiento de la fase y de la amplitud en términos de su capacidad para ser comprimidas. Estos estudios abren las puertas a futuras investigaciones sobre las características de la fase, tanto para lograr diseñar sistemas ópticos que ofrezcan mayor compresión como para mejorar el rendimiento de los algoritmos tradicionales al ser

aplicados a datos de este tipo. En la medida que las aplicaciones de la holografía digital aumenten, esperamos que esta área de investigación cobre cada vez mayor importancia.

Por otro lado, el multiplexado con máscaras binarias que proponemos tiene interesantes aplicaciones más allá de la reducción de volumen, permitiendo la posibilidad de implementar técnicas de estenografía y seguridad óptica, usando las máscaras aleatorias binarias como llaves adicionales, o para ocultar información dentro de un holograma.

Finalmente, exploramos lo que es tal vez el área más novedosa de todas las aquí expuestas, es decir, la visualización de información holográfica. Este tipo de métodos, estuvieron limitados por los moduladores de luz y sus reducidas prestaciones, pero actualmente son foco de un renovado interés, gracias a los avances en las tecnologías necesarias para su desarrollo. Tras demostrar el proceso básico para reconstruir hologramas digitales usando un modulador espacial de fase, pasamos revista a dos técnicas comunes de generación de hologramas por computadora, y demostramos una novedosa combinación de ambas. La técnica propuesta introduce la denominada fase aleatoria optimizada, la cual permite un aumento en la velocidad de generación de hologramas por computadora, dando lugar a la posibilidad de producir videos holográficos en tiempo real. Esta técnica además tiene aplicaciones más allá de la demostrada en la generación de hologramas 2D. Como uno de los últimos resultados de nuestra investigación, encontramos que estas fases tienen las características adecuadas para lograr una reducción del ruido en la encriptación [97] superior a la lograda hasta ahora. Entre las perspectivas adicionales, resultantes de la investigación aquí presentada, encontramos la generación de volúmenes de fase aleatoria optimizados, extendiendo así el concepto de las fases optimizadas a la generación de hologramas de datos tridimensionales. Por otro lado, existen técnicas alternativas de generación de hologramas, las cuales pueden ser aplicadas a la optimización de fases aleatorias. También se debe explorar la extensión a la generación de hologramas de Fresnel del concepto de las fases optimizadas.

La sección final de la tesis muestra como reconstruir ópticamente información holográfica con múltiples longitudes de onda, capacidad que complementa la exposición sobre la holografía digital a color, y que es requisito en sistemas de proyección de escenas naturales con medios holográficos. Adicionalmente, aprovechamos el sistema experimental desarrollado para mostrar, por primera vez, la reconstrucción óptica de

datos holográficos comprimidos, dando un soporte experimental adicional a las técnicas ya propuestas en el capítulo 3.

Como perspectiva integradora de todo lo expuesto en estas conclusiones, planeamos avanzar en la implementación de un sistema de proyección holográfica de datos encriptados a color en tiempo real, aplicación la cual demostraría el manejo de contenidos holográficos de forma completa, incluyendo su registro, procesamiento, encriptación, compresión y finalmente proyección.

Además, la investigación en el área de proyección holográfica es de gran utilidad con miras a exploraciones futuras de nuevas técnicas, como la óptoestimulación neuronal, la corrección de aberraciones con elementos ópticos adaptativos, la microscopia holográfica y la manipulación con pinzas ópticas.

Reconocimientos, publicaciones y participación en eventos

Reconocimientos.

Durante la realización de esta tesis doctoral se lograron los siguientes reconocimientos

Diciembre 2017	Coinvestigador en el proyecto "Manejo seguro y eficiente de la información por medio de la luz" premiado como investigación de más impacto del año 2017, Alcaldía de Medellín, Medellín, Colombia
Octubre 2017	Mención de honor en el premio Ciencia y Solidaridad, categoría Ciencias Físicas y Naturales, Fundación Alejandro Ángel Escobar, Bogotá, Colombia
Noviembre 2016	Premio de la Sociedad Americana de Óptica al estudiante 2016 durante la IX Reunión iberoamericana de Óptica, Pucón, Chile.
Mayo 2016	Premio a la mejor presentación en poster durante el XII Taller de Óptica y Fotónica, Buenos Aires, Argentina

Adicionalmente, el artículo "*Optical field data compression by opto-digital means*, Journal of Optics 18, 125701 (2016)" fue nombrado como "IOPselect" de IOPscience y seleccionado como "Highlights of 2016" de Journal of Optics, por su novedad e impacto.

Publicaciones.

Las contribuciones novedosas desarrolladas durante el transcurso de mi beca doctoral dieron lugar a las siguientes publicaciones.

[1] Alexis Jaramillo, John Fredy Barrera, Santiago Montoya, Alejandro Mira-Agudelo, **Alejandro Vélez Zea**, Roberto Torroba: *Improved decryption quality with a random reference beam cryptosystem*. Optics and Lasers in Engineering 09/2018; 112:119-127., DOI:10.1016/j.optlaseng.2018.09.006

[2] **Alejandro Velez Zea,** John Fredy Barrera, Roberto Torroba: *Optimized random phase encryption.* Optics Letters, 06/2018. Early posting DOC ID: 332951.

[3] Sorayda Trejos, John Fredy Barrera, **Alejandro Velez Zea**, Myrian Tebaldi, Roberto Torroba: *Compression of multiple 3D color scenes with experimental recording and reconstruction.* Optics and Lasers in Engineering 01/2018; 110:18-23. DOI:10.1016/j.optlaseng.2018.04.020

[4] **Alejandro Velez Zea**, John Fredy Barrera, Roberto Torroba: *Optimized random phase only holograms.* Optics Letters 02/2018; 43(4). DOI: 10.1364/OL.43.000731

[5] Alexis Jaramillo, John Fredy Barrera, **Alejandro Vélez Zea**, Roberto Torroba: *Fractional optical cryptographic protocol for data containers in a noise-free multiuser environment*. Optics and Lasers in Engineering 01/2018; 102:119-125., DOI:10.1016/j.optlaseng.2017.10.008

[6] **Alejandro Velez Zea**, John Fredy Barrera, Roberto Torroba: *Cryptographic salting for security enhancement of double random phase encryption schemes*. Journal of optics 08/2017; 19(10)., DOI:10.1088/2040-8986/aa8738

[7] **Alejandro Velez Zea**, John Fredy Barrera, Roberto Torroba: *Cross-talk free selective reconstruction of individual objects from multiplexed optical field data*. Optics and Lasers in Engineering 08/2017; 100:90-97., DOI:10.1016/j.optlaseng.2017.07.014

[8] **Alejandro Velez Zea,** John Fredy Barrera, Roberto Torroba: *Experimental optical encryption of grayscale information*. Applied Optics 07/2017; 56(21):5883-5889., DOI:10.1364/AO.56.005883

[9] **Alejandro Velez Zea**, John Fredy Barrera, Roberto Torroba: *Innovative speckle noise reduction procedure in optical encryption*. Journal of optics 03/2017; DOI:10.1088/2040-8986/aa6526

[10] **Alejandro Velez Zea**, John Fredy Barrera, Sorayda Trejos, Myrian Tebaldi, Roberto Torroba: *Optical field data compression by opto-digital means*. Journal of optics 12/2016; 18(12):125701., DOI:10.1088/2040-8978/18/12/125701

[11] **Alejandro Velez Zea**, John Fredy Barrera, Roberto Torroba: *Customized data container for improved performance in opt*ical cryptosystems*. Journal of optics 11/2016; 18(12)., DOI:10.1088/2040-8978/18/12/125702

[12] Alexis Jaramillo, John Fredy Barrera, **Alejandro Velez Zea**, Roberto Torroba: *Experimental analysis of a joint free space cryptosystem*. Optics and Lasers in Engineering 08/2016; 83:126-130., DOI:10.1016/j.optlaseng.2016.03.010

[13] Sorayda Trejos, John Fredy Barrera, **Alejandro Velez Zea**, Myrian Tebaldi, Roberto Torroba: *Optical approach for the efficient data volume handling in experimentally encrypted data*. Journal of optics 04/2016; 18(6)., DOI:10.1088/2040-8978/18/6/065702

[14] **Alejandro Velez Zea**, John Fredy Barrera Ramirez, Roberto Torroba: *Three-dimensional joint transform correlator cryptosystem*. Optics Letters 02/2016; 41(3):599-602., DOI:10.1364/OL.41.000599

[15] **Alejandro Velez Zea**, John Fredy Barrera-Ramírez, Roberto Torroba: *One-step reconstruction of assembled 3D holographic scenes*. Optics & Laser Technology 11/2015; 75., DOI:10.1016/j.optlastec.2015.06.028

Participación en eventos.

Algunos de los resultados presentes en este trabajo de tesis fueron presentados los siguientes eventos y conferencias nacionales e internacionales

[1] **Alejandro Velez Zea**, John Fredy Barrera, Roberto Torroba, "Reconstruccion en un solo paso de escenas holograficas 3d" EEOFF-TOPFOT, Corrientes, (Argentina) 2015. Expositor.

[2] Sorayda Trejos, **Alejandro Velez Zea**, John Fredy Barrera, Myrian Tebaldi, Roberto Torroba, "Reducción del volumen de información holográfica" XIV Encuentro nacional de óptica (XIV ENO) y V Conferencia Andina y del Caribe en Optica y sus Aplicaciones (IV CANCOA) Santiago de Cali, (Colombia) 2015. Coautor.

[3] Alexis Jaramillo, John Fredy Barrera, **Alejandro Velez Zea**, Roberto Torroba, "Criptografía óptica usando un sistema sin lentes" XIV Encuentro nacional de óptica (XIV ENO) y V Conferencia Andina y del Caribe en Óptica y sus Aplicaciones (IV CANCOA) Santiago de Cali, (Colombia) 2015. Coautor.

[4] Alexis Jaramillo, John Fredy Barrera, **Alejandro Velez Zea**, Roberto Torroba, "Implementación experimental de un sistema de encriptación fraccionario" XIV Encuentro nacional de óptica (XIV ENO) y V Conferencia Andina y del Caribe en Óptica y sus Aplicaciones (IV CANCOA) Santiago de Cali, (Colombia) 2015. Coautor.

[5] **Alejandro Velez Zea**, Alexis Jaramillo, John Fredy Barrera, Roberto Torroba, "Encriptación óptica con propagación en el espacio libre" EEOFF-TOPFOT, Buenos Aires, (Argentina) 2016. Expositor.

[6] **Alejandro Velez Zea**, John Fredy Barrera, Roberto Torroba, "Multiplexing three-dimensional optically encrypted data" Frontiers in Optics & Laser Science Conference, Rochester, NY (Estados Unidos) 2016. Expositor

[7] Alexis Jaramillo, John Fredy Barrera, **Alejandro Velez Zea**, Roberto Torroba, "Sistema de encriptación fraccional con recuperación libre de ruido" IX Iberoamerican Meeting on Optics and XII Iberoamerican Meeting on Optics, Lasers and Applications (RIAO / OPTILAS), Pucon (Chile) 2016. Coautor.

[8] **Alejandro Velez Zea**, John Fredy Barrera, Roberto Torroba, "Multiplexado axial de datos encriptados en el dominio de Fresnel" IX Iberoamerican Meeting on Optics and XII Iberoamerican Meeting on Optics, Lasers and Applications (RIAO / OPTILAS), Pucon, (Chile) 2016. Expositor.

[9] Sorayda Trejos, **Alejandro Velez Zea**, John Fredy Barrera, Myrian Tebaldi, Roberto Torroba, "Reducción del volumen de datos holograficos mediante escalado óptico" IX Iberoamerican Meeting on Optics and XII Iberoamerican Meeting on Optics, Lasers and Applications (RIAO / OPTILAS), Pucon (Chile) 2016. Coautor.

[10] John Fredy Barrera, **Alejandro Velez Zea**, Roberto Torroba, "Noise-free recovering optical encryption using information containers" IX Iberoamerican Meeting on Optics and XII Iberoamerican Meeting on Optics, Lasers and Applications (RIAO / OPTILAS), Pucon (Chile) 2016. Coautor.

[11] **Alejandro Velez Zea**, Sorayda Trejos, John Fredy Barrera, Myrian Tebaldi, Roberto Torroba, “Técnicas ópticas de compresión de datos holográficos” IV Jornadas de Investigación, Transferencia y Extensión de la Facultad de Ingeniería, La Plata (Argentina) 2017.Coautor.

[12] Roberto Torroba, **Alejandro Velez Zea**, John Fredy Barrera. “Noise analysis and reduction applied to optically encrypted data codes”, 24rd ICO conference. Tokyo (Japon) 2017. Coautor.

[13] Alexis Jaramillo, John Fredy Barrera, **Alejandro Velez Zea**, Roberto Torroba, “Manejo seguro de múltiples datos con recuperación libre de ruido en el dominio fraccionario” XV Encuentro nacional de Optica (XIV ENO) y VI Conferencia andina y del caribe en Optica y sus Aplicaciones (VI CANCOA), Bucaramanga (Colombia) 2017.

[14] Sorayda Trejos, John Fredy Barrera, **Alejandro Velez Zea**, Myrian Tebaldi, Roberto Torroba, “Compresión de campos ópticos de objetos tridimensionales a color” XV Encuentro nacional de Optica (XIV ENO) y VI Conferencia andina y del caribe en Optica y sus Aplicaciones (VI CANCOA), Bucaramanga (Colombia) 2017.

[15] **Alejandro Velez Zea**, John Fredy Barrera, Roberto Torroba, “Optimized random phase only holograms in the Fresnel domain” SPIE Optics+Photonics, San Diego (Estados Unidos) 2018. Autor.

[16] Alexis Jaramillo, John Fredy Barrera, Santiago Montoya, Alejandro Mira Agudelo, **Alejandro Velez Zea**, Roberto Torroba, “Experimental noise-free information recovery via reference beam encryption” SPIE Optics+Photonics, San Diego (Estados Unidos) 2018. Autor.

Proceedings

Algunos de los trabajos presentados en los eventos arriba descritos fueron acompañados de proceedings.

[1] **Alejandro Velez Zea**, John Fredy Barrera, Roberto Torroba, "Optimized random phase only holograms in the Fresnel domain," Proc. SPIE 10751, Optics and Photonics for Information Processing XII, 1075105 (7 September 2018); doi: 10.1117/12.2319842

[2] John Alexis Jaramillo Osorio, John Fredy Barrera Ramírez, Santiago Montoya, Alejandro Mira-Agudelo, **Alejandro Velez Zea**, Roberto Torroba, "Experimental noise-free information recovery via reference beam encryption," Proc. SPIE 10721, Active Photonic Platforms X, 107212E (19 September 2018); doi: 10.1117/12.2321349

[3] Roberto Torroba, **Alejandro Velez Zea**, John Fredy Barrera, "Noise Analysis and reduction applied to optically encrypted data codes" 24th ICO conference, Tokyo (Japon) 2017.

[4] **Alejandro Velez Zea**, Sorayda Trejos, John Fredy Barrera, Myrian Tebaldi, Roberto Torroba, "Tecnicas opticas de compresión de datos holográficos." IV Jornadas de Investigación, Transferencia y Extensión de la Facultad de Ingeniería pp 247-252 (La Plata, 2017).

[5] **Alejandro Velez Zea**, Roberto Torroba, John Fredy Barrera, "Multiplexing three-dimensional optically encrypted data", Frontiers in Optics 2016, OSA Technical Digest (online) (Optical Society of America, 2016), paper JW4A.45.

[6] Roberto Torroba, **Alejandro Velez Zea**, John Fredy Barrera, "Experimental scrambling technique to strengthen optical encryption", XXIII Congress of the International Commission for Optics (ICO 23): enlightening the future, Proceedings of ICO XXIII, paper Opt_Imag_63_87 (2014).

Referencias

1. D. Gabor, "A new microscopic principle," Nature 161, 777-778 (1948).
2. J. W. Goodman y R. W. Lawrence, "Digital image formation from electronically detected holograms," Appl. Phys. Lett. 11, 77-79 (1967).
3. E. N. Leith y J. Upatnieks, "Reconstructed Wavefronts and Communication Theory*," J. Opt. Soc. Am. 52, 1123 (1962).
4. I. Yamaguchi y T. Zhang, "Phase-shifting digital holography," Opt. Lett. 22, 1268 (1997).
5. J. Liu y T. Poon, "Two-step-only quadrature phase-shifting digital holography," Opt. Lett. 34, 250 (2009).
6. X. Ma, G. R. Arce, y Y. Li, "Optimal 3D phase-shifting masks in partially coherent illumination.," Appl. Opt. 50, 5567-76 (2011).
7. U. Schnars y W. P. O. Jüptner, "Digital recording and numerical reconstruction of holograms," Meas. Sci. Technol. 13, R85-R101 (2002).
8. M. King, "Measurement and application of dynamic range for holographic storage media.," Appl. Opt. 11, 791-797 (1972).
9. A. Velez Zea, J. F. Barrera-Ramírez, y R. Torroba, "One-step reconstruction of assembled 3D holographic scenes," Opt. Laser Technol. 75, 146-150 (2015).
10. E. N. Leith y J. Upatnieks, "Wavefront Reconstruction with Diffused Illumination and Three-Dimensional Objects*," J. Opt. Soc. Am. 54, 1295 (1964).
11. H. I. Bjelkhagen y E. Mirlis, "Color holography to produce highly realistic three-dimensional images," Appl. Opt. 47, A123 (2008).
12. P. Ferraro, S. De Nicola, G. Coppola, A. Finizio, D. Alfieri, y G. Pierattini, "Controlling image size as a function of distance and wavelength in Fresnel-transform reconstruction of digital holograms," Opt. Lett. 29, 854 (2004).
13. A. V. Oppenheim y J. S. Lim, "The Importance of Phase in Signals," Proc. IEEE 69, 529-541 (1981).
14. I. Yamaguchi, K. Yamamoto, G. a Mills, y M. Yokota, "Image reconstruction only by phase data in phase-shifting digital holography.," Appl. Opt. 45, 975-

983 (2006).

15. M. May y M. Françon, "Correlation and information processing using speckles," J. Opt. Soc. Am. 66, 1275 (1976).

16. P. Refregier y B. Javidi, "Optical image encryption based on input plane and Fourier plane random encoding," Opt. Lett. 20, 767 (1995).

17. B. Javidi, "Experimental demonstration of the random phase encoding technique for image encryption and security verification," Opt. Eng. 35, 2506 (1996).

18. T. Nomura y B. Javidi, "Optical encryption using a joint transform correlator architecture," Opt. Eng. 39, 2031 (2000).

19. A. Lugt, "Signal detection by complex spatial filtering," Inf. Theory, IEEE Trans. 139-145 (1964).

20. C. S. Weaver y J. W. Goodman, "A Technique for Optically Convolving Two Functions," 5, 1248-1249 (1966).

21. J. W. Goodman, *Introduction to Fourier Optics*, McGraw-Hill physical and quantum electronics series (W. H. Freeman, 2005).

22. J. W. Goodman, *Speckle Phenomena in Optics: Theory and Applications* (Roberts & Company, 2007).

23. E. Rueda, J. F. Barrera, R. Henao, y R. Torroba, "Optical encryption with a reference wave in a joint transform correlator architecture," Opt. Commun. 282, 3243-3249 (2009).

24. G. Situ y J. Zhang, "Double random-phase encoding in the Fresnel domain," Opt. Lett. 29, 1584 (2004).

25. C. La Mela y C. Iemmi, "Optical encryption using phase-shifting interferometry in a joint transform correlator," Opt. Lett. 31, 2562–2564 (2006).

26. J. M. Vilardy, M. S. Millán, y E. Pérez-Cabré, "Nonlinear optical security system based on a joint transform correlator in the Fresnel domain," Appl. Opt. 53, 1674 (2014).

27. V. NAMIAS, "The Fractional Order Fourier Transform and its Application to Quantum Mechanics," IMA J Appl Math 25, 241-265 (1980).

28. R. Torres, P. Pellat-Finet, y Y. Torres, "Fractional convolution, fractional correlation and their translation invariance properties," Signal Processing 90, 1976-1984 (2010).

29. D. Mendlovic y H. M. Ozaktas, "Fractional Fourier transforms and their optical implementation: I," J. Opt. Soc. Am. A 10, 1875 (1993).

30. H. M. Ozaktas y D. Mendlovic, "Fractional Fourier transforms and their optical implementation II," J. Opt. Soc. Am. A 10, 2522 (1993).

31. G. Unnikrishnan, J. Joseph, y K. Singh, "Optical encryption by double-random phase encoding in the fractional Fourier domain.," Opt. Lett. 25, 887-889 (2000).

32. a W. Lohmann y D. Mendlovic, "Fractional joint transform correlator.," Appl. Opt. 36, 7402-7 (1997).

33. G. Unnikrishnan, J. Joseph, y K. Singh, "Optical encryption by double-random phase encoding in the fractional Fourier domain," Opt. Lett. 25, 887 (2000).

34. J. M. Vilardy, Y. Torres, M. S. Millán, y E. Pérez-Cabré, "Generalized formulation of an encryption system based on a joint transform correlator and fractional Fourier transform," J. Opt. 16, 125405 (2014).

35. A. Jaramillo, J. F. Barrera, A. V. Zea, y R. Torroba, "Fractional optical cryptographic protocol for data containers in a noise-free multiuser environment," Opt. Lasers Eng. 102, 119-125 (2018).

36. A. Carnicer, M. Montes-Usategui, S. Arcos, y I. Juvells, "Vulnerability to chosen-cyphertext attacks of optical encryption schemes based on double random phase keys," Opt. Lett. 30, 1644 (2005).

37. X. Peng, P. Zhang, H. Wei, y B. Yu, "Known-plaintext attack on optical encryption based on double random phase keys," Opt. Lett. 31, 1044 (2006).

38. R. W. Gerchberg y W. O. Saxton, "A practical algorithm for the determination of phase from image and diffraction plane pictures," Optik (Stuttg). 35, 237-246 (1972).

39. J. F. Barrera, C. Vargas, M. Tebaldi, R. Torroba, y N. Bolognini, "Known-plaintext attack on a joint transform correlator encrypting system," Opt. Lett. 35, 3553 (2010).

40. H. Tashima, M. Takeda, H. Suzuki, T. Obi, M. Yamaguchi, y N. Ohyama, "Known plaintext attack on double random phase encoding using fingerprint as key and a method for avoiding the attack.," Opt. Express 18, 13772-13781 (2010).

41. J. R. Fienup, "Phase retrieval algorithms: a personal tour [Invited].," Appl. Opt. 52, 45-56 (2013).

42. C. Zhang, M. Liao, W. He, y X. Peng, "Ciphertext-only attack on a joint transform correlator encryption system," Opt. Express 21, 28523 (2013).

43. X. Liu, J. Wu, W. He, M. Liao, C. Zhang, y X. Peng, "Vulnerability to ciphertext-only attack of optical encryption scheme based on double random phase encoding," Opt. Express 23, 18955 (2015).

44. G. Li, W. Yang, D. Li, y G. Situ, "Cyphertext-only attack on the double random-phase encryption: Experimental demonstration," Opt. Express 25, 8690-8697 (2017).

45. M. Liao, W. He, D. Lu, y X. Peng, "Ciphertext-only attack on optical cryptosystem with spatially incoherent illumination: From the view of imaging through scattering medium," Sci. Rep. 7, 1-9 (2017).

46. O. Katz, P. Heidmann, M. Fink, y S. Gigan, "Non-invasive single-shot imaging through scattering layers and around corners via speckle correlations," Nat. Photonics 8, 784-790 (2014).

47. C. Guo, I. Muniraj, y J. T. Sheridan, "Phase-retrieval-based attacks on linear-canonical-transform-based DRPE systems," Appl. Opt. 55, 4720 (2016).

48. J. M. Vilardy, M. S. Millán, y E. Pérez-Cabré, "Improved decryption quality and security of a joint transform correlator-based encryption system," J. Opt. 15, 025401 (2013).

49. K. Falaggis, A. H. R. Andrade, J. G. G. Luna, C. G. Ojeda, y R. Porras-Aguilar, "Optical encryption with protection against Dirac delta and plain signal attacks," Opt. Lett. 41, 4787-4790 (2016).

50. P. Kumar, J. Joseph, y K. Singh, "Impulse attack-free four random phase mask encryption based on a 4-f optical system.," Appl. Opt. 48, 2356-2363 (2009).

51. R. Morris y K. Thompson, "Password security: a case history," Commun. ACM 22, 594-597 (1979).

52. A. V. Zea, J. F. Barrera, y R. Torroba, "Cryptographic salting for security enhancement of double random phase encryption schemes," J. Opt. 19, 105703 (2017).

53. J. F. Barrera, E. Rueda, C. Rios, M. Tebaldi, N. Bolognini, y R. Torroba, "Experimental opto-digital synthesis of encrypted sub-samples of an image to improve its decoded quality," Opt. Commun. 284, 4350-4355 (2011).

54. J. F. Barrera, A. Vélez, y R. Torroba, "Experimental multiplexing protocol to encrypt messages of any length," J. Opt. (United Kingdom) 15, (2013).

55. J. F. Barrera, A. Mira, y R. Torroba, "Optical encryption and QR codes: Secure and noise-free information retrieval," Opt. Express 21, 5373 (2013).

56. J. F. Barrera, A. Mira-Agudelo, y R. Torroba, "Experimental QR code optical encryption: noise-free data recovering," Opt. Lett. 39, 3074 (2014).

57. I. S. Reed y G. Solomon, "Polynomial Codes Over Certain Finite Fields," J. Soc. Ind. Appl. Math. 8, 300-304 (1960).

58. A. V. Zea, J. F. Barrera, y R. Torroba, "Customized data container for improved performance in optical cryptosystems," J. Opt. (United Kingdom) 18, (2016).

59. J. C. Dainty, *Laser speckle and related phenomena* (1975).

60. J. F. Barrera, A. Vélez, y R. Torroba, "Experimental scrambling and noise

reduction applied to the optical encryption of QR codes," Opt. Express 22, 20268 (2014).

61. A. V. Zea, J. F. Barrera, y R. Torroba, "Innovative speckle noise reduction procedure in optical encryption," J. Opt. (United Kingdom) 19, (2017).

62. A. V. Zea, J. F. Barrera, y R. Torroba, "Experimental optical encryption of grayscale information," Appl. Opt. 56, 5883 (2017).

63. F. J. Harris, "On the use of windows for harmonic analysis with the discrete Fourier transform," Proc. IEEE 66, 51-83 (1978).

64. E. Tajahuerce y B. Javidi, "Encrypting three-dimensional information with digital holography," Appl. Opt. 39, 6595 (2000).

65. A. V. Zea, J. F. B. Ramirez, y R. Torroba, "Three-dimensional joint transform correlator cryptosystem," Opt. Lett. 41, (2016).

66. D. A. Huffman, "A Method for the Construction of Minimum-Redundance Codes," Proc. I.R.E. 40, 1098-1101 (1952).

67. J. Ziv y A. Lempel, "A universal algorithm for sequential data compression," IEEE Trans. Inf. Theory 23, 337-343 (1977).

68. T. J. Naughton, Y. Frauel, B. Javidi, y E. Tajahuerce, "Compression of digital holograms for three-dimensional object reconstruction and recognition.," Appl. Opt. 41, 4124-4132 (2002).

69. J. W. Goodman y A. M. Silvestri, "Some Effects of Fourier-domain Phase Quantization," IBM J. Res. Dev. 14, 478-484 (1970).

70. W. J. Dallas, "Phase Quantization — a Compact Derivation," 10, 1970-1971 (1970).

71. W. J. Dallas, "Phase Quantization in Holograms — a Few Illustrations," 10, 674-676 (1971).

72. W. J. Dallas y a W. Lohmann, "Phase quantization in holograms-depth effects.," Appl. Opt. 11, 192-4 (1972).

73. G. A. Mills y I. Yamaguchi, "Effects of quantization in phase-shifting digital holography," Appl. Opt. 44, 1216 (2005).

74. G. K. Wallace, "The JPEG Still Picture Compession Standard," Commun. ACM 34, 31-44 (1991).

75. R. Shahnaz, J. F. Walkup, y T. F. Krile, "Image compression in signal-dependent noise.," Appl. Opt. 38, 5560-7 (1999).

76. S. Trejos, J. F. Barrera, A. Velez, M. Tebaldi, y R. Torroba, "Optical approach for the efficient data volume handling in experimentally encrypted data," J. Opt.

18, 065702 (2016).

77. F. A. Jenkins y H. E. White, *Fundametals of Optics* (2001).

78. A. Velez, J. F. Barrera, S. Trejos, M. Tebaldi, y R. Torroba, "Optical field data compression by opto-digital means," J. Opt. (2016).

79. A. V. Zea, J. F. Barrera, y R. Torroba, "Cross-talk free selective reconstruction of individual objects from multiplexed optical field data," Opt. Lasers Eng. 100, 90-97 (2018).

80. J. a Davis y D. M. Cottrell, "Random mask encoding of multiplexed phase-only and binary phase-only filters.," Opt. Lett. 19, 496-498 (1994).

81. B. E. Usevitch, "A tutorial on modern lossy wavelet image compression: foundations\nof JPEG 2000," IEEE Signal Process. Mag. 18, 1-14 (2001).

82. B. R. Brown y A. W. Lohmann, "Complex Spatial Filtering with Binary Masks," Appl. Opt. 5, 967 (1966).

83. M. Makowski, "Minimized speckle noise in lens-less holographic projection by pixel separation," Opt. Express 21, 29205 (2013).

84. P. Memmolo, I. Esnaola, a. Finizio, M. Paturzo, P. Ferraro, y a. M. Tulino, "SPADEDH: a sparsity-based denoising method of digital holograms without knowing the noise statistics," Opt. Express 20, 17250 (2012).

85. Y. Takaki y M. Yokouchi, "Speckle-free and grayscale hologram reconstruction using time-multiplexing technique," Opt. Express 19, 7567 (2011).

86. D. E. Smalley, Q. Y. J. Smithwick, V. M. Bove, J. Barabas, y S. Jolly, "Anisotropic leaky-mode modulator for holographic video displays," Nature 498, 313-317 (2013).

87. F. Yaraş, H. Kang, y L. Onural, "State of the art in holographic displays: A survey," IEEE/OSA J. Disp. Technol. 6, 443-454 (2010).

88. M. Kronrod, N. S. Merzlyakov, y L. P. Yaroslavskii, "Computer synthesis of transparency holograms.," Sov. Phys. Tech. Phys. 17, 329 (1972).

89. Z. Zhang, Z. You, y D. Chu, "Fundamentals of phase-only liquid crystal on silicon (LCOS) devices," Light Sci. Appl. 3, 1-10 (2014).

90. H. Zhang, J. Xie, J. Liu, y Y. Wang, "Elimination of a zero-order beam induced by a pixelated spatial light modulator for holographic projection," Appl. Opt. 48, 5834 (2009).

91. A. V. Zea, J. F. Barrera Ramirez, y R. Torroba, "Optimized random phase only holograms," Opt. Lett. 43, 731 (2018).

92. T. Ito y K. Okano, "Color electroholography by three colored reference lights

simultaneously incident upon," 12, 4320-4325 (2004).

93. M. Oikawa, T. Shimobaba, T. Yoda, H. Nakayama, A. Shiraki, N. Masuda, y T. Ito, "Time-division color electroholography using one-chip RGB LED and synchronizing controller," Opt. Express 19, 12008 (2011).

94. A. Jesacher, S. Bernet, y M. Ritsch-marte, "Colour hologram projection with an SLM by exploiting its full phase modulation range," 22, 252-262 (2014).

95. M. Makowski, I. Ducin, M. Sypek, A. Siemion, A. Siemion, J. Suszek, y A. Kolodziejczyk, "Color image projection based on Fourier holograms.," Opt. Lett. 35, 1227-1229 (2010).

96. S. Trejos, J. F. B. Ramirez, A. V. Zea, M. Tebaldi, y R. Torroba, "Compression of multiple 3D color scenes with experimental recording and reconstruction," Opt. Lasers Eng. 110, (2018).

97. A. Velez Zea, J. F. Barrera Ramirez, y R. Torroba, "Optimized random phase encryption," Opt. Lett. 43, 3558 (2018).

Índice de figuras